Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

Magazine

13e jaargang 2015 nr. 3

Nationale veiligheid en crisisbeheersing

Thema: Herijking vitale infrastructuur

Overige onderwerpen

INHOUD

Het Magazine nationale veiligheid en crisisbeheersing is een tweemaandelijkse uitgave van de Nationaal Coördinator Terrorismebestrijding en Veiligheid van het Ministerie van Veiligheid en Justitie.

Het blad informeert, signaleert en biedt een platform aan bestuurders en professionals over beleidsontwikkeling, innovatie, uitvoering en evaluatie ten aanzien van nationale veiligheid en crisisbeheersing.

De uitgever is het niet noodzakelijkerwijs eens met de inhoud van gepubliceerde bijdragen. De verantwoordelijkheid en aansprakelijkheid voor de inhoud van de artikelen berust bij de auteurs.

Foto Omslag:
Shutterstock

Wat is vitaal?

Heeft u al uw eigen drone in huis? Kost bijna niets meer. Ideaal voor het maken van luchtfoto's van uw vakantiebestemming. Of om pakketjes te bezorgen, geen last meer van files. Drones die boven een grote brand hangen geven hulpverleners een goed beeld van de situatie. Maar wat als diezelfde drones worden gebruikt om een gas- of waterleiding op te blazen? En daarmee op een relatief eenvoudige manier deze vitale sectoren aan te tasten? Nieuwe technieken met ongekende nieuwe kansen, maar ook nieuwe bedreigingen.

Dick Schoof
Nationaal Coördinator Terrorismebestrijding en Veiligheid

Kijken we naar de vitale infrastructuur, dan valt de grote onderlinge afhankelijkheid op. En dus de impact als er iets uitvalt of verstoord raakt. Een langdurige stroomuitval – zoals onlangs in Noord-Holland – raakt bijvoorbeeld veel processen: transport, energielevering, toegang tot internet, betalingsverkeer. En die onderlinge afhankelijkheid is door toenemende digitalisering nóg groter geworden.

Kort samengevat: nieuwe technieken, steeds grotere onderlinge afhankelijkheden en toenemende betekenis van vitale bedrijven. Dat maakt dat een herijking van tien jaar beleid voor de bescherming van de vitale infrastructuur nodig was. Anders gezegd: opnieuw bepalen wat vitaal is voor Nederland en kijken of deze infrastructuur weerbaar genoeg is tegen alle dreigingen die we vandaag de dag kennen.

Kernvraag was: wat is de economische, fysieke en sociale impact op de samenleving als deze sector uitvalt? Met andere woorden: stel dat er in een vitale sector uitval of verstoring is … wat is dan minimaal de hoeveelheid euro's schade, het aantal slachtoffers en hoe groot is de overlast voor personen en andere vitale sectoren? En hoe prioriteren we onze schaarse middelen om deze vitale sectoren weerbaarder te maken om incidenten te voorkómen of de gevolgen ervan te beperken?

Samen met partners van overheid en bedrijfsleven hebben we een lijst gemaakt wat vitaal is en daarbij een onderscheid gemaakt op basis van impact. Om een lange opsomming in dit voorwoord te voorkomen verwijs ik u gemakshalve naar het artikel in dit magazine, waarin de vitale processen en diensten staan. En u vindt in dit magazine ook volop aandacht voor regionale, nationale en internationale ontwikkelingen en gevolgen voor de vitale infrastructuur. Belicht door zowel de overheid, bedrijven als de wetenschap. We maken publiek-private "roadmaps": afspraken wie wat doet en wanneer. En zoals uw navigatiesysteem vitaal is voor het bereiken van uw vakantiebestemming, moet de *roadmap* ons gezamenlijk naar het juiste doel leiden: een veilige en weerbare infrastructuur in Nederland.

Ik wens u veel leesplezier.

EEN VERANDERENDE WERELD VRAAGT OM EEN MEE VERANDEREND BELEID

De herijking vitale infrastructuur Nederland

Op 27 maart 2015 werd duidelijk hoe afhankelijk onze samenleving is van elektriciteit. Door een stroomstoring in Noord-Holland kwamen een miljoen huishoudens zonder stroom te zitten. Daarnaast vielen verkeerslichten uit, kwamen treinen, metro's en trams stil te staan en konden vliegtuigen niet meer landen op Schiphol. In het getroffen gebied waren het mobiele telefoonverkeer en het elektronische betalingsverkeer ook verstoord en een gedeelte van het bedrijfsleven kwam stil te liggen (Bron: nieuwsbericht NOS, 27 maart).

Richard Addae, Jetske Hebbink en Sven Hamelink
Directie Weerbaarheidsverhoging, NCTV, Ministerie van Veiligheid en Justitie

Het waarborgen van de continuïteit van vitale infrastructuur is van gezamenlijk belang voor zowel de vitale (veelal private) organisaties als voor de samenleving. Onder vitale infrastructuur verstaan we producten, diensten en de onderliggende processen die, als zij uitvallen, grootschalige maatschappelijke ontwrichting kunnen veroorzaken. Overheid en vitale organisaties werken in Nederland daarom samen aan de bescherming van de vitale infrastructuur. Door de vele betrokken partijen, de benodigde integrale benadering, technologische ontwikkelingen en de gelaagdheid en verwevenheid van vitale processen is dit een dynamisch en complex domein. De samenleving is afhankelijker geworden van vitale infrastructuur terwijl de maatschappelijke acceptatie van de uitval van een dergelijke infrastructuur juist is afgenomen. De infrastructuur is onder andere afhankelijker geworden van ICT-systemen en van elektriciteit en daarmee ook voor (moedwillige) cyberincidenten. Vitale processen zijn daarnaast dermate verknoopt dat cascade-effecten moeilijk zijn te voorspellen en ook groter van omvang zijn bij uitval van één proces. Vitale organisaties en de Rijksoverheid onderkennen dit mede op basis van ketenanalyses bij vitale organisaties.

De Minister van Veiligheid en Justitie heeft namens het Kabinet aan de Tweede Kamer in 2013 toegezegd om het beleid rondom de bescherming van vitale infrastructuur te herijken. De herijking heeft geleid tot een nieuwe geprioriteerde lijst van wat aangemerkt moet worden als vitale infrastructuur in Nederland met meer focus. In plaats van een sectorale benadering is gefocust op de relevante processen onderliggend aan de producten en diensten en is de vitale infrastructuur in Nederland anno 2015 ook gedefinieerd in processen. Ook heeft het inzicht opgeleverd met betrekking tot de belangrijkste risico's, dreigingen, kwetsbaarheden en mate van weerbaarheid van deze infrastructuur. Bovendien is er (meer) aandacht voor de implementatie: waar daar aanleiding toe is, zijn afspraken gemaakt om zowel de fysieke als digitale weerbaarheid te verhogen. De afspraken zijn vastgelegd in zogenaamde roadmaps. Met behulp van de gezamenlijke doestelling *Continuïteit van de samenleving* wordt daarnaast implementatie in de Veiligheidsregio's gerealiseerd. De herijking legt met dit alles de basis voor een geactualiseerd en aangescherpt structureel beleid rondom vitale infrastructuur in Nederland. Inmiddels is de beoordeling van wat vitaal is voor Nederland zo goed als afgerond. In april zijn de resultaten van de beoordeling in de Voortgangsbrief Nationale Veiligheid aan de Tweede Kamer gepresenteerd.

Een eenduidige definitie en identificatie van de vitale infrastructuur voor Nederland anno 2015 en een daarop toegerust weerbaarheid bestendigend of -verhogend beleid zijn van groot belang voor de nationale veiligheid. Daartoe is de mate van vitaliteit bezien op basis van criteria en grenswaarden voor maatschappelijke ontwrichting die gelden voor alle publieke en (semi) private partners. De criteria zijn ontwikkeld aan de hand van de beoordelingssystematiek van de Nationale Risicobeoordeling (NRB) uit de Strategie Nationale Veiligheid. Tijdens de herijking is een integrale beoordeling van de mate van vitaliteit uitgevoerd, waarbij de gevolgen van uitval van de in 2009 benoemde vitale sectoren (gedefinieerd in 2005, aangescherpt in 2009) zijn beoordeeld op economische, fysieke en sociale impact.

Verder zal in 2015 actie worden ondernomen om mogelijke nieuwe vitale infrastructuur te identificeren. Daarnaast wordt er ingezet op het beter ontsluiten en waar nodig ontwikkelen van instrumenten voor de vitale infrastructuur. Strategische allianties zullen worden aangegaan om intersectorale informatie-uitwisseling en kennisborging te realiseren.

Door de herijking kunnen andere weerbaarheidsverhogende instrumenten gericht(er) worden ingezet. Zo zal vitale infrastructuur worden opgenomen binnen de crisisstructuren en krijgt deze bijzondere aandacht binnen de Nationale Academie voor Crisisbeheersing. Verder wordt de vitale infrastructuur opgenomen in de Producten- en Diensten Catalogus van het Nationaal Cybersecurity Centrum. Het (kunnen) aanwijzen van vertrouwensfuncties wordt ook bezien in relatie tot de categorieën van vitaal. Dit geldt eveneens voor het Alerteringssysteem Terrorismebestrijding (ATb), dat overigens van onverkorte toepassing blijft op de huidige daarbij aangesloten sectoren. Ten slotte ligt het voor de hand dat de mate van vitaliteit wordt gehanteerd als afbakening in toekomstige trajecten en beleid en ook aansluit op gerelateerde trajecten zoals Vitaal en Kwetsbaar uit het Deltaprogramma, de Europese Netwerk en Informatiebeveiligingsrichtlijn (NIB-richtlijn) en de Wet Meldplicht en Gegevensverwerking Cybersecurity.

De herijking heeft, dankzij de gezamenlijke inspanningen van de relevante publieke en private partners, geleid tot een actueel en eenduidig zicht op wat vitaal is voor onze samenleving, waarbij de impact op de samenleving centraal staat: één integrale lijst vitale infrastructuur. Om te kunnen prioriteren bij onder andere incidenten en om maatwerk bij weerbaarheidsverhogende maatregelen mogelijk te maken, is onderscheid gemaakt tussen de categorie A en B zodat recht wordt gedaan aan de diversiteit binnen de vitale infrastructuur.

CATEGORIE A

In deze categorie staat de infrastructuur die bij verstoring, aantasting of uitval de ondergrenzen van minstens één van de vier impactcriteria voor categorie A raakt:

- economische gevolgen: meer dan ca. 50 miljard euro schade of ca. 5.0 % daling reëel inkomen;
- fysieke gevolgen: meer dan 10.000 personen dood, ernstig gewond of chronisch ziek;
- sociaal maatschappelijke gevolgen: meer dan 1 miljoen personen ondervinden emotionele problemen of ernstig maatschappelijke overlevingsproblemen;
- cascadegevolgen: uitval heeft als gevolg dat minimaal twee andere sectoren uitvallen.

CATEGORIE B

In deze categorie staat de infrastructuur die bij verstoring, aantasting of uitval de ondergrenzen van minstens één van de drie impactcriteria voor categorie B raakt:

- economische gevolgen: meer dan ca. 5 miljard euro schade of ca. 1.0 % daling reëel inkomen;
- fysieke gevolgen: meer dan 1.000 personen dood, ernstig gewond of chronisch ziek;
- sociaal maatschappelijke gevolgen: meer dan 100.000 personen ondervinden emotionele problemen of ernstig maatschappelijke overlevingsproblemen.

DE NIEUWE LIJST MET VITALE INFRASTRUCTUUR

Processen	Cat.	Product, dienst of locatie	Sector	Ministerie
Landelijk transport en distributie elektriciteit	A	Elektriciteit	Energie	Economische Zaken
Regionale distributie elektriciteit	B			
Gasproductie Landelijk transport en distributie gas	A	Aardgas		
Regionale distributie gas	B			
Olievoorziening	A	Olie		
Internettoegang en dataverkeer	PM[1]		ICT/Tel	Economische Zaken
Spraakdiensten (mobiel en vast)				
Satelliet				
Tijd- en plaatsbepaling (satelliet)				
Drinkwatervoorziening	A	Drinkwater	Drinkwater	Infrastructuur en milieu
Keren en beheren waterkwantiteit	A	• (deel van de) primaire waterkeringen • (deel van de) regionale waterkeringen[2]	Water	Infrastructuur en milieu
Vlucht- en vliegtuigafhandeling	B	Mainport Schiphol	Transport	Infrastructuur en milieu
Scheepvaartafwikkeling	B	Mainport Rotterdam		
Grootschalige productie/verwerking en/of opslag (petro)chemische stoffen	B	(petro)chemische industrie	Chemie	Infrastructuur en milieu
Opslag, productie en verwerking nucleair materiaal	A	Nucleaire industrie	Nucleair	Infrastructuur en milieu
Toonbankbetalingsverkeer	B	Betalingsverkeer	Financieel	Financiën
Massaal giraal betalingsverkeer	B			
Hoogwaardig betalingsverkeer tussen banken	B			
Effectenverkeer	B			
Communicatie met en tussen hulpdiensten met behulp van 112 en C2000	B	Handhaving van de openbare orde en veiligheid	OOV[3]	Veiligheid en Justitie
Inzet politie	B			
Beschikbaarheid van betrouwbare basisinformatie over personen en organisaties, informatie-uitwisseling van basisinformatie en beschikbaarheid van datasystemen waarvan meerdere overheidsorganisaties voor hun functioneren afhankelijk zijn.	B	Digitale overheid[4]	Openbaar Bestuur[5]	Binnenlandse Zaken en Koninkrijksrelaties

De NCTV heeft een Handboek Herijking Vitaal opgesteld met nadere informatie over de herijking en een toelichting op de vitale processen. Voor dit Handboek of vragen over de bescherming van de vitale infrastructuur kunt u contact opnemen met het Programma Vitaal via vitaal@nctv.minvenj.nl.

[1] Herijking Telecom volgt na besprekingen met sector en het ministerie van Economische zaken in voorjaar 2015.
[2] Op dit moment wordt in samenwerking met de waterschappen gekeken naar welke regionale waterkeringen vitaal zijn, conform de methodiek vitaliteits-beoordeling 2014.
[3] Vitaliteitsbeoordeling defensie wordt nog uitgevoerd in 2015.
[4] Op dit moment wordt in samenwerking met de betrokken ministeries en uitvoeringsorganisaties binnen deze clusters bekeken welke processen en systemen van de digitale overheid vitaal zijn, conform de methodiek vitaliteitsbeoordeling 2014. De processen en systemen zullen, na een beoordeling van de (financiële) consequenties, gehoord het Nationaal Beraad Digitale Overheid, worden benoemd.
[5] Vitaliteitsbeoordeling diplomatieke communicatie wordt nog uitgevoerd in 2015.

De betrouwbaarheid van het toekomstige elektriciteitsnet

In deze bijdrage wordt ingegaan op de ontwikkelingen die de betrouwbaarheid beïnvloeden van het net voor transport en distributie van elektriciteit in Nederland. Dit landelijke net is een vitale infrastructuur van categorie A, zoals aangegeven in de Voortgangsbrief Nationale Veiligheid. Er worden enkele oplossingsrichtingen aangegeven om de elektriciteitsvoorziening meer robuust te maken. Ook worden enkele lessen getrokken uit de recente grote storing van 27 maart 2015 toen een grootschalige onderbreking van de elektriciteitsvoorziening plaatsvond in een groot deel van Noord-Holland en een klein deel van Flevoland als gevolg van een kortsluiting op het 380kV hoogspanningsstation van TenneT in Diemen.

Peter Vaessen
Segment Director Future Transmission Grids,
DNV GL-Energy (peter.vaessen@dnvgl.com)[1]

ONTWIKKELINGEN ELEKTRICITEITSVOORZIENING

Onze hedendaagse maatschappij is in hoge mate afhankelijk geworden van een betrouwbare elektriciteitsvoorziening door de toegenomen interacties met andere infrastructuren, zoals informatievoorziening, transport en de waterhuishouding. Deze afhankelijkheid zal steeds verder toenemen en met de verschuiving van de "brandstofmix" – vervanging van andere energiebronnen met elektriciteit en de toename van het aandeel variabele duurzame bronnen – spreken we van een zogenaamde "double risk trend". Investeerders, eigenaren en bedrijfsvoerders van netten zijn in toenemende mate onzeker of het systeem geschikt is voor het leveren van betrouwbare elektrische energie in de juiste hoeveelheid, op het juiste moment en de juiste plaats. Daarnaast speelt de vraag of het net robuust en flexibel genoeg is om in geval van fouten en onderbrekingen weer snel operationeel te zijn. Dit alles uiteraard tegen acceptabele maatschappelijke kosten.

Factoren die bijdragen aan de "double risk" trend en het moeilijker maken om "in control" te blijven zijn:

- een toenemende ontkoppeling van opwekking en gebruik van elektriciteit;
- de grootschalige (duurzame) opwekking vindt op grote afstand plaats, meer gedistribueerd en dieper in de haarvaten van het elektriciteitsnet;
- de toenemende leeftijd van componenten, verschillende technologie-generaties - van mechanisch tot digitaal – in combinatie met het zwaarder belasten ervan;
- grote verschillen in het planningsproces voor opwekking en de transport en distributie infrastructuur. Zo kan lokale duurzame opwekking in een tijdsbestek van maanden worden gerealiseerd, grotere windparken in enkele jaren terwijl realisatie van nieuwe hoogspanningslijnen tientallen jaren kan vergen;
- toenemende elektriciteitshandel tussen landen leidt tot meer fluctuerende transporten over grotere afstanden;
- een afname van de beschikbaarheid van balancerend vermogen door het sluiten van grote (conventionele) energiecentrales;
- de snelheid waarmee nieuwe technologieën worden geïntroduceerd en waarvan de effecten en betrouwbaarheid op de lange duur onvoldoende bekend zijn (bijvoorbeeld gelijkstroomverbindingen, vermogenselektronica, stuur- en regel installaties).

Het elektriciteitsnet is in een snel tempo aan het veranderen van een, weliswaar erg groot, relatief eenvoudig fysisch systeem in de richting van een complex niet-lineair digitaal regelsysteem. Deze veranderingen brengen ook risico's met zich mee, vooral op het gebied van stabiliteit en in het bijzonder de cyber-veiligheid, aangezien een steeds groter gedeelte van de elektriciteitsvoorziening via internet toegankelijk wordt gemaakt voor besturing, bewaking en zelfs onderhoud. Zie ter illustratie de "in-game" afbeelding van het computerspel GTA 5, waarin op realistische wijze onderdelen van de elektrische infrastructuur zijn nagebouwd en zelfs te saboteren zijn, met alle gevolgen van dien voor de virtuele spelwereld.

ROBUUSTE OPLOSSINGSRICHTINGEN

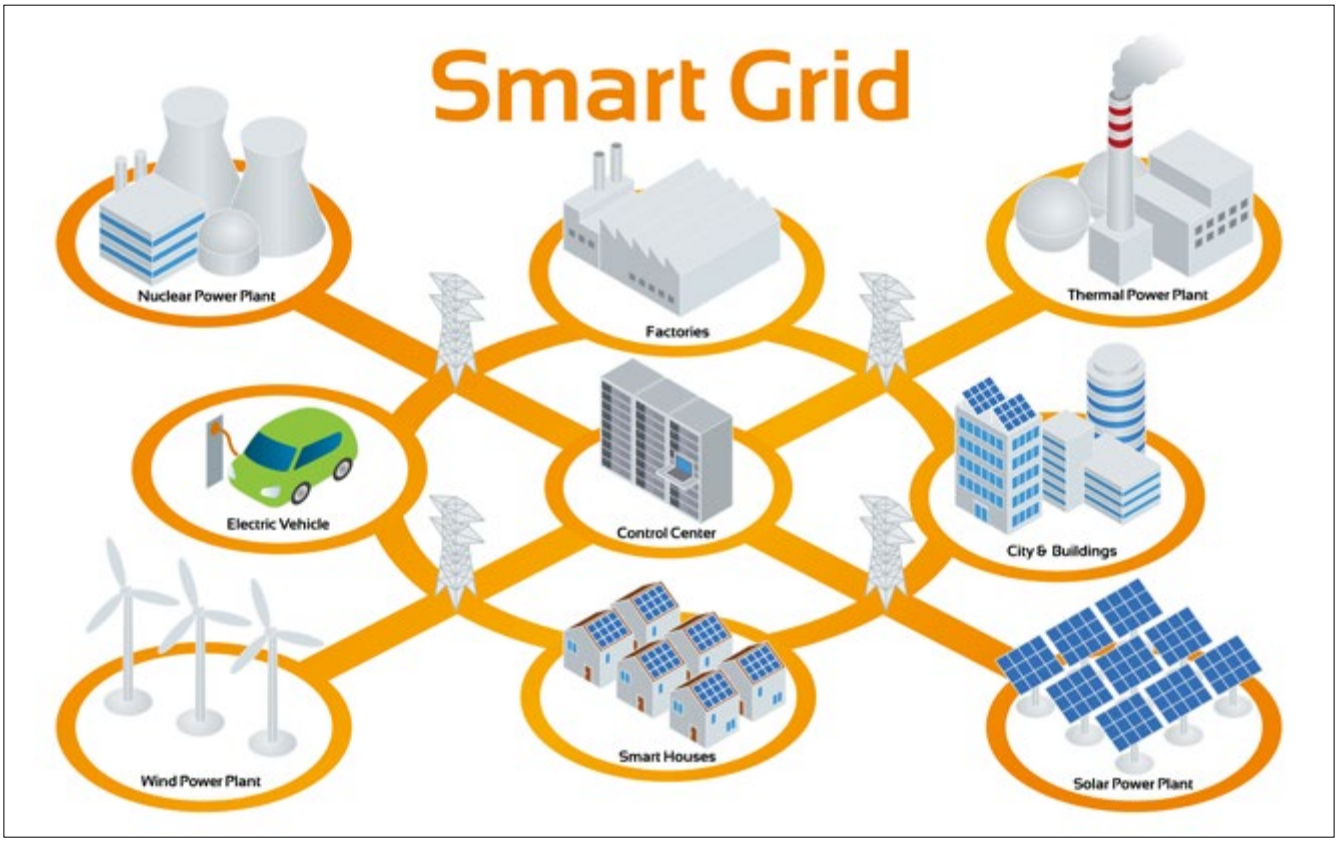
Mede door de hiervoor geschetste ontwikkelingen is het noodzakelijk dat de visie op variabele duurzame opwekking zoals zon en wind veranderd van 'lastig in te passen in de bestaande markten en bedrijfsvoering' tot een van 'supporter/ondersteuner van het elektriciteitsnet'. Dit laatste wordt werkelijkheid door de nieuwe mogelijkheden die de vermogens elektronische interfaces (*inverters*, ofwel 'omvormers') van de duurzame opwekkers hebben. Het elektriciteitsnet wordt aangepast aan de duurzame opwekking, in plaats van dat de duurzame opwekking zich moet aanpassen aan het net. Deze paradigmaverschuiving helpt ook mee om de verschillende netwerkcodes en wet- en regelgeving in de verschillende landen van de EU te harmoniseren, aangezien de (on)mogelijkheden van de duurzame opwekkers het uitgangspunt zijn en niet de verschillende manieren van bedrijfsvoering van het net.

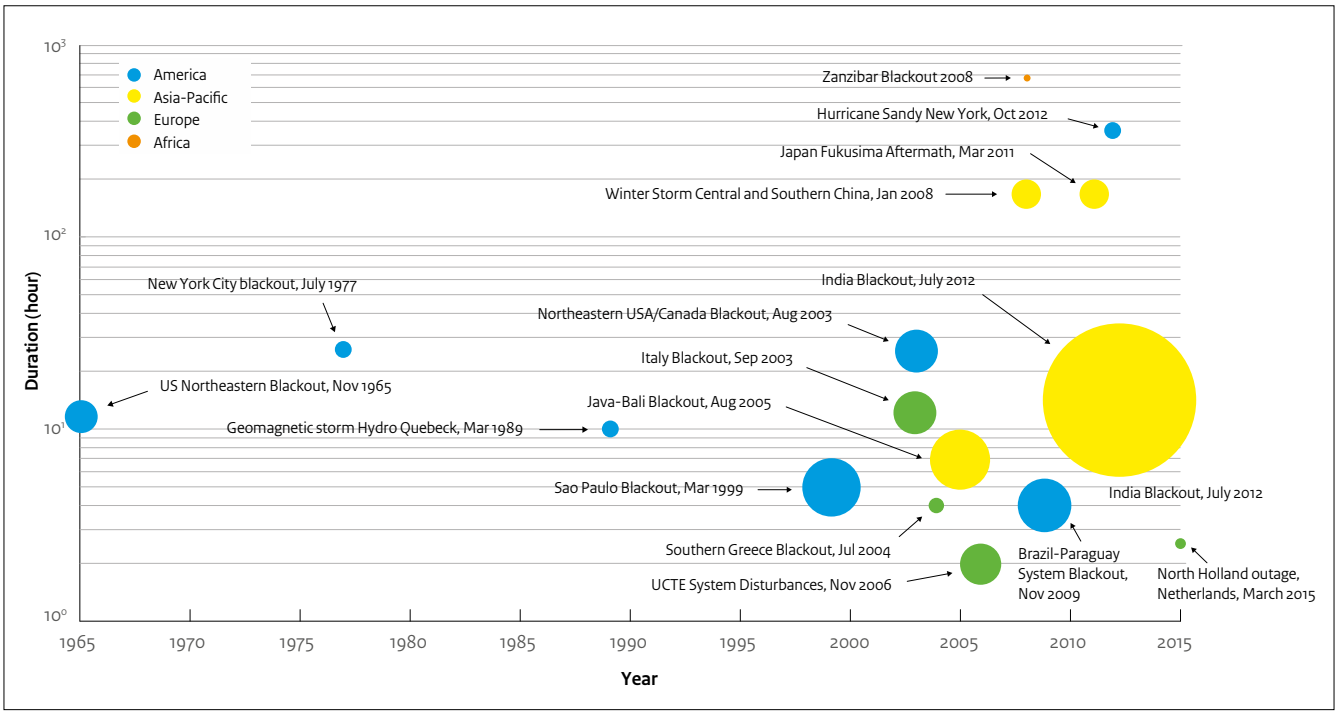
[1] DNV GL is een bundeling van de expertise van KEMA, Garrad Hassan, DNV en GL Renewables Certification. DNV GL levert wereldwijd erkende test-, inspectie- en adviesdiensten aan de energie waardeketen (www.dnvgl.com/energy).

Oplossingsrichtingen en technologieën die bijdragen aan het flexibiliseren en robuust maken van het elektriciteitsnet zijn:

- uitbreiding van het aantal elektriciteitsverbindingen tussen landen, omdat dit bijdraagt aan de vergroting van de transportcapaciteit tussen regio's en hierdoor de markt en inpassing van meer grootschalige duurzame energie faciliteert;
- meer installaties die in staat zijn het vermogen gericht te sturen in het elektriciteitsnet om congestie ('verstopping' van het hoogspanningsnet vanwege capaciteitstekort) en overbelasting te voorkomen. Voorbeelden hiervan zijn zogenaamde fase verschuivende transformatoren en snel regelbare gelijkstroomverbindingen;
- nauwkeurigere voorspelmethoden voor zowel het aanbod als de vraag van elektriciteit;
- ontwikkelen en benutten van de mogelijkheden van inverters die zorgen voor spanningsondersteuning en stabiliteitsverbetering van het net;
- introduceren van aggregatie van gedistribueerde duurzame opwekking en vraag, in combinatie met voldoende netgekoppelde energieopslag met verschillende regelsnelheden voor betere balancering;
- vaststellen van dynamische belastbaarheid van hoogspanningslijnen en kabels, bijvoorbeeld gebaseerd op de weersituatie waardoor deze effectiever benut kunnen worden;
- aanbrengen van flexibele verbindingen (via gelijkstroom) en samenwerken met lokale mini- en micronetten waardoor een deels ontkoppeld en robuuster net ontstaan.

Door deze maatregelen ontstaat een zogenaamd hybride elektriciteitsnet dat een combinatie bevat van verschillende technologieën zoals wissel- en gelijkstroom, passieve en actieve regelingen en conventionele en duurzame opwekking, zowel groot als klein. Een dergelijk net is robuust en flexibel en is in staat om de gebruikers ook in de toekomst van betaalbare, betrouwbare en duurzaam opgewekte elektriciteit te voorzien.





Overzicht grote stroomstoringen tot en met 2012 inclusief die van Noord Holland

LESSEN RECENTE STROOMSTORING

De Nederlandse elektriciteitsvoorziening is een van de meest betrouwbare ter wereld met een gemiddelde beschikbaarheid van 99.996%, dit komt overeen met slechts 20 minuten per jaar niet-beschikbaar zijn. Een onderbreking van de elektriciteitsvoorziening op de schaal zoals plaatsvond op 27 maart jl. als gevolg van een storing in het 380kV station Diemen is erg zeldzaam. De laatste grote storing in Nederland was die van 1997, waarbij de provincie Utrecht getroffen werd. De onderbreking van 27 maart trof circa één miljoen huishoudens en een aantal grootverbruikers en vitale infrastructuren zoals Schiphol en delen van het spoorwegnet. De figuur geeft een overzicht van de grootste stroomstoringen tot en met 2012 waarin ook de storing van Noord Holland is opgenomen. Dergelijke onderbrekingen worden meestal veroorzaakt door een combinatie van technisch falen en menselijk handelen waarbij op een kritiek moment een fout of defect optreedt dat onjuist geïnterpreteerd wordt en een hierop een passende, maar verkeerde, oplossingsrichting gekozen wordt, zo ook bij deze storing.

Naast de aanpak gericht op het voorkomen van onderbrekingen door verbeteringen in techniek, procedures en werkinstructies en vergroten van het kennisniveau van bevoegde personen, krijgt ook het snel herstellen, het creëren van "*fallback/last resort*" middelen en het inbouwen van meer flexibiliteit steeds meer aandacht. Essentieel hierbij is een betere coördinatie en samenwerking tussen alle betrokken organisaties en instellingen die een rol spelen bij de elektriciteitsvoorziening, wat overigens in toenemende mate een Europese dimensie heeft. Daarnaast zijn risico-inschattingen, het beoordelen van nieuwe technologie en het vaststellen van de benodigde mate van automatisering van de bedrijfsvoering belangrijke aandachtsgebieden hierbij.

REFERENTIES

Reliability of Future Power Grids. Position paper DNV GL.
Cyber security for electricity utilities, DNV GL 10-2014.

Computerspel GTA 5: Wat is reëel en wat is virtueel?

Landelijke gasvoorziening is “A-vitaal”

Han Fennema
CEO Gasunie

“Landelijk transport en distributie van gas op landelijke schaal” is samen met “gasproductie” door het kabinet in het kader van het project “herijkijking vitaal” ingedeeld in de hoogste categorie. De uitkomsten van de herijkingsoperatie zijn in april dit jaar in een voortgangsbrief door minister Van der Steur aan de Tweede Kamer gestuurd. De indeling in categorie A is logisch. Onze samenleving draait in belangrijke mate op aardgas en een grootschalige verstoring van de gasvoorziening heeft daarmee direct ontwrichtende gevolgen. Huizen, kantoren en ziekenhuizen worden verwarmd met gas, heel veel mensen koken op gas en we willen graag allemaal een warme douche. Daarnaast gaat er veel gas naar de industrie, waar het wordt gebruikt in het productieproces van allerhande producten. Ook wordt gas getransporteerd naar centrales om er stroom mee op te wekken. Er is sprake van een grote onderlinge afhankelijkheid tussen gas en elektriciteit. Grootschalige verstoring van de landelijke stroomvoorziening brengt de gasvoorziening in gevaar en andersom is dat ook het geval. Alleen daarom al is het logisch dat ook de landelijke elektriciteitsvoorziening in de hoogste categorie is ingedeeld. De regionale distributie van gas is eveneens belangrijk, maar het verschil is dat een verstoring daar beperkt is tot een deel van Nederland. Het transport door de regionale bedrijven als Enexis en Alliander is daarom door de overheid ingedeeld in de één na hoogste categorie. Een grote verstoring in het net van Gasunie of in de toevoer vanuit producenten heeft effect in heel Nederland en zelfs ook daarbuiten. Nederland is (nog steeds) een belangrijke exporteur van gas naar het omringende buitenland.

Gasunie produceert zelf geen gas en handelt er ook niet in. Producenten en handelaren maken gebruik van onze infrastructuur. Deze bestaat in de eerste plaats uit het landelijk gastransportnet van onze dochter GTS BV, maar voor de landelijke gasvoorziening is ook andere infrastructuur van Gasunie van belang. Voorraden vloeibaar gas (LNG) worden bijvoorbeeld opgeslagen in de GATE terminal op de Maasvlakte, waarin Gasunie een belang van 50% heeft en in de ondergrondse gasopslag van EnergyStock, een 100% dochter van Gasunie. Voor extreem koude winterdagen is de Randstad afhankelijk van een reservevoorraad vloeibaar gas in onze zogenoemde “peak shaver”. Het samenstel van deze infrastructuur is, samen met de Nederlandse gasproductie, nodig voor een betrouwbare, ongestoorde gasvoorziening. De transportinfrastructuur bestaat uit meer dan leidingen. Om het gas in de vereiste kwaliteit en met de juiste druk van A naar B te krijgen, hebben we compressorstations, mengstations en stikstofinstallaties verspreid door Nederland. We vinden het als burgers normaal dat er altijd warm water uit de kraan komt, maar dat is geen vanzelfsprekendheid. Op landelijke schaal werken er 1800 mensen bij Gasunie om de gasstromen letterlijk in goede banen te leiden. Gelukkig gaat dit bijna altijd goed, zo goed zelfs dat we ons niet altijd realiseren wat de gevolgen zijn als dit plotseling niet meer het geval zou zijn.

Overzicht gastransportnetwerk © Gas Transport Services

Naast veiligheid staat bij Gasunie daarom ook security hoog in het vaandel. Ook voor de herijkingsoperatie was Gasunie reeds als “vitaal” aangemerkt. Dit brengt verantwoordelijkheden en verplichtingen met zich mee. De overheid verwacht dat we ons, in het belang van de samenleving, adequaat beschermen tegen ongewenste invloeden van buitenaf of vanuit de onderneming zelf.

Vanwege dit laatste worden medewerkers met bepaalde functies gescreend, alvorens ze hun functie kunnen uitoefenen. De externe bedreigingen kunnen divers van aard zijn en variëren van fysieke bedreigingen van de infrastructuur tot hackers van onze complexe computersystemen. Er kunnen criminelen achter zitten, maar ook terroristen. Voor de fysieke beveiliging van de infrastructuur kent Gasunie een classificatiesysteem op grond waarvan keuzes worden gemaakt ten aanzien van de beveiliging: wel of geen (dubbele) hekken, camera's etc. Met name de aandacht voor "cyber" heeft de laatste jaren een enorme vlucht genomen. Ook Gasunie besteedt veel aandacht aan de beveiliging van haar IT-systemen. Als onderneming uit de categorie "A -vitaal" zijn we nauw aangesloten bij het Nationaal Cyber Security Centrum (NCSC). Vanuit de Commissie Vitale Infrastructuur van het VNO-NCW werken we samen met bedrijven uit dezelfde categorie. Het is belangrijk dat bedrijven die van vitaal belang zijn voor de samenleving intensief samenwerken met de overheid op het gebied van security. In Nederland lopen we voorop met vormen van zogenoemde Publiek Private Samenwerking (PPS). Het NCSC is daarvan een goed voorbeeld. In het managementteam zit ook iemand vanuit en namens de vitale bedrijven. Juist omdat vitale bedrijven en de overheid een gezamenlijk belang dienen, kan zo kennis worden gedeeld en verder worden ontwikkeld. Ook kan er in geval van een cybercrisis snel en adequaat worden gereageerd.

Gasunie is een onderneming en zoals elk bedrijf streven we naar rendement. Gastransport is echter "gereguleerd", in die zin dat de tarieven worden vastgesteld door de toezichthouder, de ACM. We moeten er van uit kunnen gaan dat de genomen maatregelen die als consequentie van het overheidsbeleid uit een oogpunt van publiek belang noodzakelijk zijn, ook de goedkeuring kunnen wegdragen van de toezichthouder en verdisconteerd mogen worden in de tarieven. Security is natuurlijk een kostenpost die niet direct geld oplevert. Alle maatregelen die genomen worden, hebben ten doel te voorkomen dat er ontwrichtende verstoringen optreden. Eigenlijk hoop je dat de genomen securitymaatregelen nooit echt nodig zijn en dat ze uit zichzelf tot gevolg hebben dat kwaadwilligen "zich er niet aan wagen". We zijn ons bewust dat de status van "A-vitaal" de lat hoog legt en dus verantwoordelijkheid met zich brengt. Het beleid blijft er daarom op gericht al die maatregelen te nemen die passend zijn bij deze status.

KNOOPPUNT IN TRANSITIE

Olie en petrochemie

Nederland vervult een belangrijke rol in de olie- en gasvoorziening van NW Europa met haar exportraffinaderijen, olie- en gasopslagcapaciteit en netwerk van olie-, chemie- en gaspijpleidingen naar België, het Verenigd Koninkrijk (VK), Frankrijk en Duitsland. De olie- en gassector is bovendien nauw verbonden met de internationale markten. In de komende decennia zal de olie- en gassector ook sterk beïnvloed worden door de voorgenomen veranderingen in de energiemix in het kader van het klimaatbeleid. Deze veranderingen zullen asymmetrisch verlopen in de zin dat een beroep op het oude (olie en gas) en het nieuwe systeem (wellicht meer elektriciteit, warmte en bio-brand en grondstoffen) er voor kunnen zorgen dat systemen naast elkaar moeten functioneren, zodat het aanwenden van "oude" infrastructuur in het nieuwe systeem belemmerd of vertraagd kan worden als bijmengen niet meer volstaat.

Prof. dr. Coby van der Linde
Hoofd Clingendael International Energy Programme

CLUSTER

Het ARA (Amsterdam, Rotterdam en Antwerpen (ARA)) vormen samen een belangrijk olie- en petrochemiecluster met verschillende verbindingen naar het Europese achterland. In Rotterdam staan vijf raffinaderijen met een destillatiecapaciteit van 58 miljoen ton.[1] Rotterdam is verbonden via ruwe oliepijpleidingen met vijf andere raffinaderijen in Antwerpen, Vlissingen en twee raffinaderijen in Duitsland. Naast deze pijpleidingen maakt Rotterdam ook deel uit van het *Central European Pipeline System* (CEPS) van de NAVO, die de raffinaderijen verbindt met militaire en civiele luchthavens. Van de raffinageproductie bestaat 85% uit allerlei brandstoffen voor auto's, vrachtwagen, vliegtuigen en scheepvaart (benzine, diesel, gasolie, stookolie en LPG), de resterende 15% bestaat uit nafta voor de petrochemische industrie, smeeroliën en bitumen (asfalt). In de haven van Rotterdam is bovendien 13.6 miljoen kubieke meter aan opslagcapaciteit, zowel voor ruwe olie als olieproducten. Van de olieproducten wordt 40% geëxporteerd naar België en Duitsland. De Nederlandse gasproductie maakt ook deel uit van dit – energie intensieve industriële – cluster en verbindt tevens regionale gasmarkten in Europa.

TRANSITIE

De ontwikkeling naar een minder koolstof-intensieve economie in Europa enerzijds en de ontwikkelingen op internationale markten anderzijds daagt het olie- en petrochemiecluster uit zich aan te passen aan een veranderende vraag en aanbod naar energie. Bijvoorbeeld de toename van wind en zonne-energie in het aanbod van elektriciteit heeft al enorme gevolgen gehad voor het aantal bedrijfsuren van gascentrales (piek capaciteit), terwijl de vraag naar transportbrandstoffen zoals benzine en diesel stagneert door een hogere efficiëntie van de voertuigen en de komst van elektrische en hybride aangedreven personenauto's. Verder wordt de markt voor LNG voor transport ontwikkeld (vooral voor de scheepvaart) die de vraag naar specifieke olieproducten kan aantasten. De impact van de nieuwe brandstoffen en energietechnieken werd bovendien sterker gevoeld door de lage of afwezige economische groei na de financiële en economische crisis van 2008/2009 en de gevolgen daarvan voor de vraag naar energie. Door dit complex aan veranderingen wijzigt mogelijk de economische logica (het bestaansrecht van onderdelen) van het gehele olie en petrochemisch cluster en de daaraan verbonden vitale infrastructuur en opslagcapaciteit.

INTERNATIONALE DRUK

Al ruim voor de crisis van 2008/2009 was duidelijk dat een einde was gekomen aan de expansieve periode van de economie in Europa. De groei van de vraag naar kolen, olie en gas verschoof naar Azië, met China als absolute trekker van deze ontwikkeling. Nieuwe productiecapaciteit werd vooral ontwikkeld met de opkomende Aziatische markt als belangrijkste drijfveer. In het Midden-Oosten en Azië breidde de raffinagecapaciteit en petrochemie zich uit, terwijl deze kromp in de VS en Europa. In de VS werd de sluiting van niet langer renderende raffinaderijen een halt toe geroepen door de schalierevolutie, die de productie van eerst aardgas en later ook lichte olie enorm deed toenemen. Een beleidsoverblijfsel uit de jaren zeventig verbood de export van ruwe olie, waardoor de nieuwe olieproductie alleen via het raffinageluik naar de internationale markt geëxporteerd kon worden. De benuttingsgraad van Amerikaanse raffinaderijen verbeterde enorm en bracht de consolidatie tot stilstand. De schalierevolutie zorgde er voor dat de traditionele exportmarkt voor benzine en andere olieproducten van Europese raffinaderijen opdroogde waardoor de levensvatbaarheid van veel Europese raffinaderijen verder in het geding kwam. Vooral raffinaderijen die niet geïntegreerd waren in een energie-petrochemisch industrieel cluster stonden onder druk. Inmiddels zijn er verschillende Europese raffinaderijen gesloten, omgebouwd tot opslagfaciliteiten of functioneren in een handelsportefeuille. Deze laatste worden gebruikt voor arbitrage of optionaliteit tussen de ruwe olieprijzen en de prijzen in de verschillende productmarkten en hebben een meer fluctuerend productieprofiel. Door de vraagontwikkeling in Europa, de strengere eisen aan de productspecificaties en de

[1] Havenbedrijf Rotterdam.

concurrentie met raffinaderijen in andere landen, waaronder inmiddels ook Rusland, zal de sector de productieprocessen verder moeten optimaliseren. Voor sommige raffinaderijen zal de combinatie van hogere investeringen en onzekere marktvooruitzichten betekenen dat ook zij de markt zullen moeten verlaten. Voor de energie-petrochemische clusters zullen de mogelijkheden om verder te optimaliseren iets groter zijn en kunnen zij het marktaandeel vergroten door de sluiting van anderen. Niettemin voelen zij ook de druk van de veranderingen in de internationale concurrentieverhoudingen en de stagnatie van de Europese markt.

CLUSTERLOGICA IN BEWEGING

De prijsverschillen van olie en gas tussen de VS en Europa maken de Amerikaanse markt momenteel interessanter voor investeringen in nieuwe petrochemische capaciteit. Door veranderingen in het aanbod van olie en gas in de wereld, de snelle groei van alternatieve energiebronnen en de druk vanuit het beleid om een overgang te maken van petrochemie naar *bio-based* chemie komt de verknoping van het energie en industrie cluster in een ander daglicht te staan.

De mogelijkheden om de huidige marktontwikkelingen tegemoet te treden door verdere schaalvergroting zijn klein en zal er eerder een fragmentering van markten plaatsvinden door de import van olieproducten in plaats van eigen productie, nieuwe concurrentie van *bio-based feedstocks* (zoals hout pallets en andere landbouwproducten) en het afkalven van premiummarkten, die de minder renderende deelmarkten ondersteunen. Nieuwe energiehandelsstromen komen op gang, waardoor enerzijds nieuwe vraag naar opslag en vervoer ontstaat, maar anderzijds overcapaciteit in het traditionele systeem komt. Daar nieuwe stromen initieel relatief klein zijn, wordt vaak gekozen voor vervoer over water of weg. In de VS heeft bijvoorbeeld het vervoer per trein zo een vlucht genomen dat (tijdelijk) nieuwe voordelen ontstaan ten opzichte van het pijpleidingen systeem. Het is niet uitgesloten dat de krimp van traditionele energiedragers en groei van nieuwe in Europa ook een dergelijk effect hebben omdat de omslag van het ene naar het andere systeem asymmetrisch verloopt, waardoor het hergebruik van bestaande infrastructuur op papier wel, maar in de praktijk moeilijk te realiseren is (denk bijvoorbeeld aan een warmte en een gasnet naast elkaar). De coördinatie die hiervoor nodig is ontbreekt in de huidige Europese markt. Een bijkomende complicatie voor het oliesysteem is dat het NAVO-pijpleidingennetwerk verweven is in de huidige Europese marktorganisatie. Zolang de militaire hardware steunt op olieproducten zal de strategische noodzaak om het systeem in stand te houden, blijven bestaan. Maar de commerciele logica ervan zal steeds meer onder druk komen door verdere introductie van nieuwe energiebronnen en *feedstocks*. De transitie van het ene naar het andere systeem verloopt doorgaans niet geleidelijk maar gaat gepaard met schokken als gevolg van over- en ondercapaciteit van het systeem. Het Nederlandse olie en petrochemie cluster zal enerzijds aan belang winnen door de krimp elders in Europa (en de noodzaak van voorzieningszekerheid aldaar), maar tegelijkertijd onder druk komen van de veranderingen in de energiehuishouding. Investeerders zullen geprikkeld moeten worden om èn het oude systeem intact te laten zolang het economisch en strategisch nodig is èn tegelijkertijd worden uitgedaagd de oude activiteiten te verruilen voor activiteiten die perspectief hebben in het nieuwe systeem. Daarbij is het van belang om sommige elementen van een cluster overeind te houden vanwege ketenafhankelijkheid, terwijl de commerciële rationaliteit daarvoor steeds minder wordt.

CONCLUSIE

Specialisering en verkruimeling van markten zal andere eisen stellen aan de infrastructuur, maar ook aan de marktorganisatie en regulering. Door de strategische waarde van de infrastructuur enerzijds en de veranderende commerciële waarde anderzijds zal de overheid van Nederland en omringende landen uitgedaagd worden de krimp en groei in raffinage, petrochemie en olie-infrastructuur te begeleiden met beleid om de systeemwaarde te garanderen zolang de transitie voort duurt.

De drinkwatervoorziening: *terecht top vitaal!*

In het traject "Herijking vitaal" is de drinkwatervoorziening aangeduid als top vitaal, ofwel, categorie A van vitaal. Vewin vindt dit meer dan terecht. In de onderliggende impactanalyse, waarbij onder andere is gekeken naar het scenario van een grootschalige overstroming, is bevestigd dat uitval van drinkwater tot zeer grote sociaal-maatschappelijke ontwrichting leidt. Ontwrichting in de zin van gebrek aan voldoende schoon en veilig drinkwater met grote risico's voor de volksgezondheid. Daarnaast brengt uitval van drinkwater enorme cascade-effecten teweeg. De levering van water aan onder andere ziekenhuizen, de geneesmiddelenindustrie, de voedselindustrie, energiebedrijven en de nucleaire industrie valt stil met alle gevolgen van dien. Kortom, drinkwater is randvoorwaardelijk voor het functioneren van de samenleving.

Renée Bergkamp
Directeur Vewin

Vanuit de gedachte dat er altijd voldoende drinkwater van goede kwaliteit beschikbaar moet zijn, is in de Drinkwaterwet uit 2011 al erkend en vastgelegd dat de drinkwatervoorziening een vitale publieke dienst is. Een dienst die van groot algemeen belang is en onderwerp is van specifieke overheidszorg. Voldoende en schoon drinkwater liggen immers aan de basis van een goede gezondheid. In het verlengde daarvan, kent de wet een groot aantal regels en eisen op het gebied van leveringszekerheid en continuïteit. Zo hebben drinkwaterbedrijven een wettelijke leveringsplicht. Onderdeel hiervan is de eis dat bedrijven tien dagen zelfvoorzienend moeten zijn. Dit betekent dat bij uitval van bijvoorbeeld energie of telecommunicatie, de drinkwatervoorziening gedurende tien dagen voortgezet moet kunnen worden. In de praktijk betekent dit dat bedrijven onder andere over eigen noodstroomaggregaten en voorraden brandstof moeten beschikken. En dat dit ook daadwerkelijk werkt, bleek bij de grootschalige stroomuitval van 27 maart jl. In tegenstelling tot veel andere diensten, draaide de drinkwatervoorziening gewoon door. En mocht om wat voor reden dan ook de levering van kraanwater niet meer mogelijk zijn, dan zijn bedrijven verplicht om nooddrinkwater in te zetten. Hierbij gaat het om minimaal drie liter nooddrinkwater per persoon per dag op door gemeenten aangewezen distributiepunten.

Drinkwaterbedrijven kunnen en doen veel zelf op het gebied van continuïteit maar op een aantal vlakken is echt samenwerking nodig, zoals met de veiligheidsregio's. De drinkwatersector participeert dan ook actief in het voortraject van het project Continuïteit van de samenleving. Het belangrijkste punt dat de sector wil bereiken, is de implementatie van de afspraken uit het samenwerkingsconvenant tussen de drinkwaterbedrijven en veiligheidsregio's uit 2010. De convenanten zijn bijna overal getekend maar de daadwerkelijke uitvoering en naleving zijn nog gaande of moeten nog starten. Om zaken behapbaar te houden, pleit Vewin ervoor om hierbij prioriteit te geven aan de volgende drie afspraken.

Ten eerste het goed inbedden van alarmeringsafspraken. Tijdige alarmering van drinkwaterbedrijven is van groot belang om te kunnen bepalen of de drinkwatervoorziening en daarmee de volksgezondheid in gevaar is, of dat er bijvoorbeeld acuut maatregelen getroffen moeten worden, zoals het uit bedrijf nemen van waterbekkens.

Ten tweede toegangsverlening tot het Landelijk Crisismanagement Systeem van de regio's. Toegang is van belang om bij een (mogelijke) drinkwater gerelateerde calamiteit een actueel beeld te krijgen van de situatie, maar ook voor inzage in bijvoorbeeld analyseresultaten van metingen.

Ten slotte het opstellen van draaiboeken rondom de inzet van nooddrinkwater. De inzet van nooddrinkwater vergt veel personele capaciteit, zowel van het drinkwaterbedrijf als van de politie, gemeenten en veiligheidsregio's met ieder hun eigen verantwoordelijkheden. De invulling hiervan moet in de koude fase zijn afgestemd zodat een ieder weet wat hij of zij moet doen als het moment daar is. Wie is bijvoorbeeld verantwoordelijk voor de doorlevering van nooddrinkwater aan mindervaliden? Of voor de openbare orde en veiligheid op de distributiepunten?

Op 12 juni a.s. neemt het Veiligheidsberaad een definitief besluit over de doorgang van het project. Vewin blijft ook na die datum graag intensief betrokken!

Op 12 juni heeft het Veiligheidsberaad akkoord gegeven op uitvoering van de Strategische Agenda. Dit betekent dat verder wordt gewerkt aan de drie gezamenlijke projecten waaronder Continuïteit van de samenleving.

Bewustzijn van Telekwetsbaarheid kan veiligheid vergroten

Nationale Veiligheid, slechts weinigen leggen een link met de continue beschikbaarheid van telecommunicatie. Het is toch gebruikelijk dat telefoon en internet het altijd doen. Maar is dat ook zo? Incidenten uit de afgelopen jaren hebben bewezen dat betrouwbare telecommunicatie van levensbelang kan zijn.

Peter Spijkerman
Directeur-Hoofdinspecteur Agentschap Telecom

Telecommunicatie ontwikkelt zich met grote sprongen. Het is zoveel meer gaan omvatten dan 'slechts' het overbrengen van boodschappen via de telefoon, radio of televisie. Telecommunicatie is een middel om informatie te verzamelen en te delen. Het stelt ons in staat muziek te beluisteren, betalingen te doen, routes te bepalen of ons huis te beveiligen. Maar ook bedrijfskritische processen draaien steeds vaker op draadloze communicatie. Neem de tram en de metro, de matrixborden boven de snelwegen, de zelfrijdende containerwagens in de Rotterdamse haven, het vliegverkeer op Schiphol of in de nabije toekomst zelfrijdende vrachtwagens die allemaal gebruik maken van dezelfde ether.

Telecommunicatie is in 2015 onmisbaar in ons dagelijks leven, randvoorwaardelijk voor ons welzijn, welvaart en veiligheid. De vitale functie van telecommunicatie voedt de maatschappelijke verwachtingen en aanbod creëert steeds weer nieuwe vraag naar nieuwe communicatietoepassingen. De samenleving vertrouwt volledig op veilige, vlekkeloos werkende en continu beschikbare telecommunicatiesystemen. We mogen ons gelukkig prijzen dat dat ook kan in Nederland. Veel partijen werken samen om dat mogelijk te maken. Tegelijkertijd is deze telecommunicatieketen bijzonder omvangrijk en complex. En dat maakt ons kwetsbaar, wij noemen dat Telekwetsbaarheid.

De ketting is immers zo sterk als de zwakste schakel. Bij het tot stand brengen van een verbinding van beller tot beller moet je bij die ketting globaal denken aan: van mobiel naar telecommast via bijvoorbeeld glasvezel of via een vaste draadloze verbinding naar de kern van het netwerk. En van daar weer dezelfde route in omgekeerde volgorde naar degene die je belt. Daarbij kan bijvoorbeeld ook nog een wisseling van provider voorkomen.

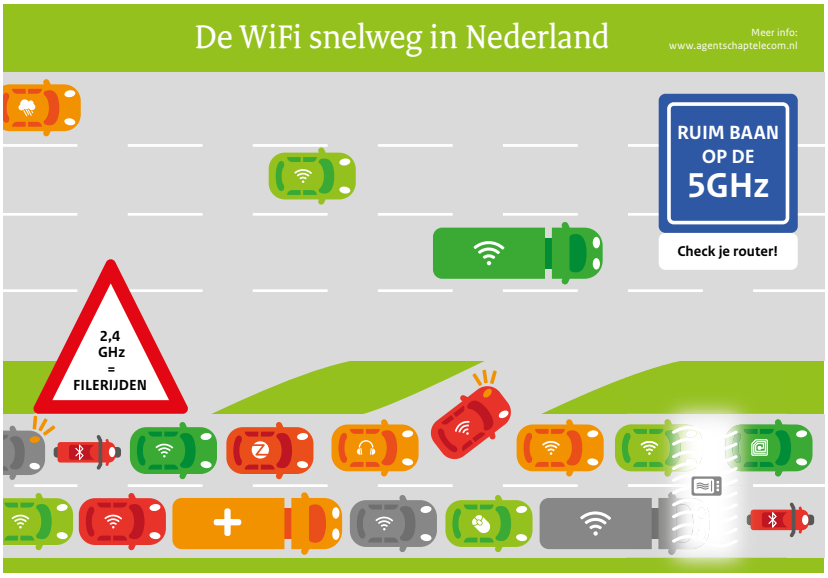
UITVAL

Als samenleving zijn wij zo afhankelijk geworden van, maar ook zo gewend geraakt aan het leven met techniek, dat we ons dat pas realiseren als alles uitvalt. Want als het netwerk er uit ligt, kan het hele bedrijf niet meer mailen, valt in ziekenhuizen de automatische registratie van patiënten uit, stoppen in fabrieken op afstand bestuurde bedrijfsprocessen en staat de continuïteit van vele diensten op het spel. Uitval van telecommunicatie kan nooit uitgesloten worden. Er zijn bijvoorbeeld technische redenen waardoor de mobiele verbinding soms niet lukt. Bijvoorbeeld omdat apparatuur uitvalt of dataverbindingen die worden verstoord (door graafschade of overmatig gebruik van WiFi). Voor de individuele consument is het al vervelend, maar voor bedrijven zijn de economische gevolgen soms enorm. En voor de samenleving komt de veiligheid in gevaar als het alarmnummer 1-1-2 of de hulpdiensten niet bereikbaar zouden zijn.

Aanbieders van telecommunicatie moeten maatregelen nemen om storingen in hun netwerken te voorkomen. Het agentschap houdt hier toezicht op. Daarnaast beheert Agentschap Telecom het loket Meldplicht Telecomwet. In 2014 zijn er bij dit loket 41 grote verstoringen gemeld, zowel van mobiele- als vaste verbindingen. Het gaat hierbij om incidenten waarbij meer dan 100.000 mensen enkele uren niet kunnen bellen of internetten, of wanneer 1-1-2 niet gebeld kan worden. Het merendeel van deze grote telecomstoringen wordt veroorzaakt door fouten in hard- en software en door menselijke fouten.

VERSTERKING KETEN

Voor Agentschap Telecom draait het om de vraag hoe de telecommunicatieketen verder versterkt kan worden, de zwakke schakels verbeterd of zelfs weggenomen. Of in het uiterste geval: hoe kunnen we er mee leren leven? In dat proces trekken wij samen op met consumenten, marktpartijen en maatschappelijke en bestuurlijke partners. Want telecommunicatie is een primaire levensbehoefte geworden en wordt beleefd als ware het een nutsvoorziening als gas/water en licht. We zijn ons alleen nog niet voldoende bewust van die afhankelijkheid, laat staan dat we voldoende maatregelen nemen om incidenten te voorkomen of te verhelpen. Of om de gevolgen van een eventuele uitval zo minimaal mogelijk te maken.



Door het massale gebruik van draadloze verbindingen in de 2,4 GHz band, adviseert Agentschap Telecom de WiFi-router over te schakelen naar de 5 GHz

GROTE STORINGEN

Dat ons verhaal niet een willekeurig rampenscenario is, is ook dit jaar meerdere keren gebleken. Zo legde een storing in maart bij een hoogspanningsstation in Diemen ook delen van het telecomnetwerk plat. Bij sommige providers kon niet of nauwelijks meer gebeld worden of lag het dataverkeer er uit. Hierbij werd weer eens onderstreept dat telekwetsbaarheid en stroomuitval nauw met elkaar verbonden zijn. Internetpagina's waren niet bereikbaar omdat servers uitvielen als gevolg van de stroomuitval. Ook geldautomaten werkten niet meer. Zelfs de nieuwsdiensten van persbureau ANP konden niet werken omdat hun server plat lag. Ook omroepen die uitzonden vanuit mediapark in Hilversum hadden problemen.

Internetknooppunt AMS-IX, een van de grootste ter wereld, kampte in mei van dit jaar met een storing die het internetverkeer in het hele land heeft getroffen. Veel sites waren moeilijk bereikbaar. De problemen ontstonden tijdens onderhoud. Hoewel de storing zelf kort duurde, hadden sommigen klanten er langer last van omdat het herstarten van verbindingen tijd kostte.

Lesson learned: (bijna) totale uitval kan iedereen overkomen. Maar wat is uw plan B?

KENNISPROGRAMMA TELEKWETSBAARHEID

Agentschap Telecom start dit jaar met het kennisprogramma Telekwetsbaarheid. Doel is bij burgers, bedrijven, instellingen en overheden de bewustwording te vergroten van de afhankelijk- en de kwetsbaarheid van telecomdiensten. Hierbij is aandacht voor de sectoren energie, transport en zorg. Maar ook voor "internet of things" – het fenomeen dat alles met alles verbonden is – en daarmee ook van elkaar afhankelijk. Ook wordt gekeken naar handelingsperspectief. Bijvoorbeeld in het WiFi-onderzoek dat recent is uitgevoerd, is duidelijk geworden waarom en waar de verbindingen haperen. Maar ook dat de oplossing, het gebruik van de 5 GHz band, nauwelijks bekend is.
Het programma richt zich ook op de veiligheidsregio's. In 2013 concludeerde de Inspectie Veiligheid en Justitie al dat uitval van telecommunicatie nauwelijks was opgenomen als risico in de continuïteitsplannen voor de crisisbeheersing vitale infrastructuur. 'Zestien van de veiligheidsregio's bleken hier niet aan te kunnen voldoen. Wanneer er al sprake is van een continuïteitplan ontbreekt het aspect uitval van nutsvoorzieningen of vitale infrastructuur.'
Agentschap Telecom assisteert de veiligheidsregio's met verbeteracties vanuit het programma Telekwetsbaarheid.
Het Kennisprogramma Telekwetsbaarheid is opgebouwd uit drie stappen:

1. onderzoek naar de belangrijkste risico's;
2. voorlichting;
3. monitoren van ontwikkelingen op het gebied van telekwetsbaarheid.

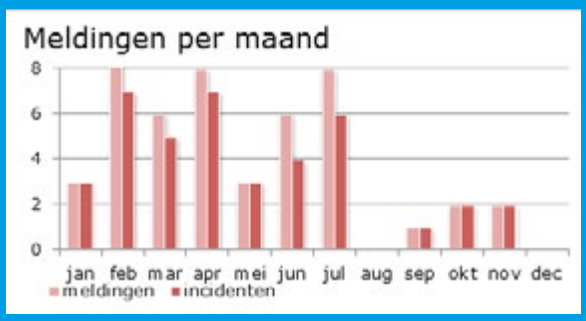
OVER AGENTSCHAP TELECOM

'Agentschap Telecom waarborgt de beschikbaarheid van moderne en betrouwbare telecommunicatie in en voor Nederland.' Het agentschap beheert namens het ministerie van Economische Zaken de ether, zodat de vele gebruikers zonder storingen met elkaar kunnen communiceren. Bijvoorbeeld omroepen, hulpdiensten, luchtverkeersleiding, aanbieders van mobiele telefonie en internet. Maar óók iedereen die gebruik maakt van WiFi, draadloze deuropeners, babyfoons etc. Agentschap Telecom wijst als een havenmeester iedereen zijn eigen plek toe in de ether. Een ingewikkeld planningsproces, waarbij rekening gehouden moet worden met nationale wensen, maar ook met internationale afspraken.

Daarnaast ziet het agentschap toe op de naleving van dit gebruik. De beschikbaarheid en betrouwbaarheid van elektronische communicatienetwerken moet zo hoog mogelijk zijn. Bedrijven, instellingen, maar ook consumenten vertrouwen erop dat ze altijd beschikbaar zijn. Wanneer dat niet zo is, ontstaat er chaos.

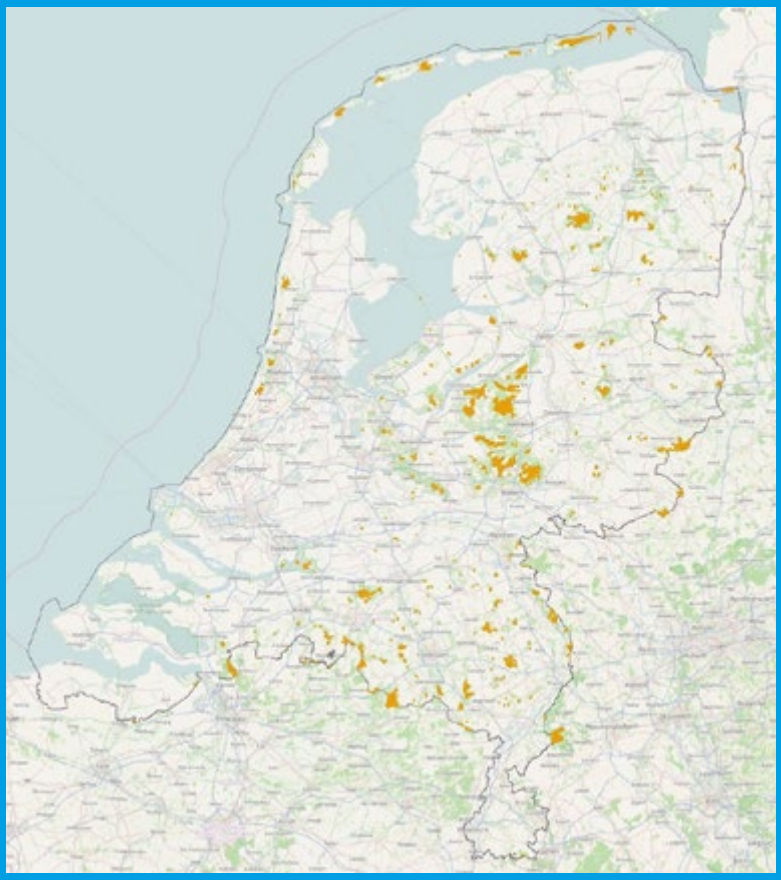
ONDERZOEK MOBIELE BEREIKBAARHEID 112

Het alarmnummer 1-1-2 en C2000 zijn onderdelen van de vitale infrastructuur. Agentschap Telecom is ervoor verantwoordelijk dat telecomproviders zorgen dat het alarmnummer 1-1-2 altijd ongestoord bereikbaar is. Onderzoek in 2014 heeft uitgewezen dat de bereikbaarheid van het alarmnummer 1-1-2 met de mobiele telefoon goed is. Providers hebben afgesproken dat wanneer het alarmnummer niet via het eigen netwerk bereikbaar is, altijd naar een wel aanwezig netwerk van een andere operator wordt overgeschakeld. Dus ook naar die van een provider waarbij je geen abonnement hebt. Dit zorgt voor die goede bereikbaarheid. Toch zijn er enkele plaatsen waar het alarmnummer met de mobiele telefoon met een minder grote waarschijnlijkheid bereikt kan worden. Dit zijn bijvoorbeeld locaties waar slechts één provider een netwerk beschikbaar heeft, dat ook nog vrij dun bedekt is. Regio's die behoefte hebben aan een nadere analyse van de bereikbaarheid van 1-1-2 in hun gebied, kunnen hierbij assistentie van het agentschap vragen om de bereikbaarheid zo mogelijk te helpen verbeteren. Dit kan met zowel technische opties (extra antennes, femto- en picocellen) als met praktische tips. De regio's kunnen daarna zelf aan de slag om, al of niet met de operators, hun telekwetsbaarheid te verminderen. En dat is het uiteindelijke ideaal, dat gebruikers van telecom zich niet alleen bewust zijn van telekwetsbaarheid, maar ook zelf hun risico's kunnen verkleinen.



In 2014 waren er 47 meldingen bij het loket Meldplicht Telecomwet over 39 grote telecomverstoringen.

- *van de 39 incidenten waren er 17 van invloed op de bereikbaarheid van 1-1-2*
- *de 39 incidenten hebben gezamenlijk tot 42 verstoringen van vitale diensten geleid: 32x binnen de telecommunicatiesector zelf, 4x omroep als rampenzender, 5x spoedeisende zorg en 1x handhaving van de openbare orde*



Gebieden in Nederland waar de verbindingswaarschijnlijkheid van de mobiele telefoon met het alarmnummer 112 lager is dan 99%

Use free lessons, manage near misses

Gelukkig is de discontinuïteit van de levering van vitale producten en diensten een zeldzaam iets in Nederland. Wat is dan de meerwaarde van het trekken van lessen uit near misses als het over het algemeen goed gaat?

Richard Addae
Directie Weerbaarheidsverhoging, NCTV, Ministerie van Veiligheid en Justitie

Dit artikel vat de resultaten samen van een onderzoek binnen vitale organisaties uit de sectoren energie, luchtvaart en chemie. Het betreft een afstudeeronderzoek voor de opleiding Integrale Veiligheidskunde.

Bij *near misses* wijkt het proces ergens af van de standaard bedrijfsvoering, maar is de continuïteit van de levering nog niet verstoord. Deze incidenten worden bewust of bij toeval gedetecteerd en gelokaliseerd waardoor organisaties nog tegenmaatregelen kunnen nemen en negatieve gevolgen voor de samenleving uitblijven. *Near misses* worden weleens afgedaan als geluk. Je zou ze echter ook als "gratis" les of advies kunnen beschouwen. Organisaties kunnen er lering uit trekken door de reactie erop, op eenzelfde wijze als ongelukken in te bedden. Dit kan door het incidentenmeldingssysteem ook voor *near misses* in te richten en de dieperliggende oorzaken te onderzoeken. En hierbij te achterhalen wat er gebeurde, hoe het kon gebeuren, en waarom het gebeurde.

De lessen die hieruit worden getrokken hebben voornamelijk betrekking op menselijk handelen. De daaruit voortkomende aanbevelingen leiden tot het nemen van maatregelen gericht op de techniek, organisatie en medewerkers. In de schakels van de veiligheidsketen kan dit zowel proactie en preventie zijn als preparatie. Een voorwaarde voor het leren van *near misses* is dat een organisatie een cultuur heeft gerealiseerd waarin open over *near misses* wordt gecommuniceerd. Hierdoor worden *near misses* ook daadwerkelijk gemeld.

Near misses komen vaker voor dan ongelukken met uitval of verstoring van een vitaal proces. Logischerwijs is uit deze grotere hoeveelheid data meer informatie over de oorzaken te halen, dan uit de enkele "echte" incidenten. Deze grotere frequentie toont ook de urgentie van een bepaalde problematiek aan. Vitale organisaties binnen onder andere de luchtvaartsector en energiesector zijn verplicht om bepaalde *near misses* te melden bij de Inspectie voor Leefomgeving en Transport en/of de Onderzoeksraad voor Veiligheid. Volgens een vitale organisatie uit de luchtvaartsector bevordert communicatie over *near misses* het vertrouwen in de organisatie, doordat de organisatie aantoonbaar aandacht besteedt aan veiligheid en aantoont weerbaar te zijn ten aanzien van dit type incidenten.

De meerwaarde van het trekken van lessen uit *near misses* bij vitale organisaties is dat het bijdraagt aan het verbeteren van het proces ondanks dat de continuïteit zelden wordt verstoord. Door het melden en vervolgens het onderzoeken van *near misses* worden *lessons learned* en aanbevelingen verkregen. Deze resultaten voeden de organisaties om keuzes te maken en het veiligheidsmanagement te verbeteren. Als vitale organisaties deze procedure omtrent *near misses* goed uitvoeren, dan verlaagt dat het risico op incidenten en bevordert het de weerbaarheid van de vitale processen.

Het onderzoek heeft geleid tot de volgende aanbevelingen aan de vitale organisaties uit de energiesector:

1. het opnemen van near misses in het veiligheidsmanagement bij alle organisaties;
2. het bevorderen van de communicatie over near misses binnen alle organisaties;
3. het delen van kennis over near misses (incidenten) tussen alle organisaties;
4. het door alle organisaties openbaar maken van informatie over near misses die zich hebben voorgedaan;
5. het realiseren van een professionele near miss cultuur op cybergebied waarin ICT near misses deel uitmaken van het veiligheidsmanagement bij alle organisaties.

Gezien de meerwaarde van het trekken van lessen uit near misses is het alle organisaties, vitaal of niet vitaal, aan te bevelen om near misses in het veiligheidsmanagement op te nemen en het melden ervan te stimuleren om zo de weerbaarheid van de organisatie te bevorderen.

Veiligheid van beide kanten

Een belangrijk onderdeel van de taak van de AIVD is het bevorderen van de nationale veiligheid. Ik zie dat als het helpen voorkomen van ernstige, doelbewuste inbreuken op de integriteit en het blijven functioneren van onze samenleving. We doen dit onder meer door onze kennis van dreiging, kwetsbaarheden en van risico's tijdig te delen.

Maar dat is maar de helft van het verhaal. Want welke belangen in het spel zijn, wat de belangrijkste kwetsbaarheden zijn en welke risico's beheersbaar, dat weten vooral de betrokken bedrijven zelf. Dit geldt zeker voor de sectoren die een vitale maatschappelijke en economische functie vervullen. Juist daarom investeren wij in de relatie met deze steunpilaren van de nationale economie. Op basis van wederzijds vertrouwen en begrip, werken we zo gezamenlijk aan de veiligheid.

Vanuit onze veiligheidsbevorderende taak zijn we natuurlijk gewend om de belangen van anderen te kennen en te behartigen, om niet alleen *voor* maar ook *samen met* hen te werken. En dat doen we graag! Gas- en elektriciteitsbedrijven en de burgerluchtvaart om er maar een paar te noemen, zijn dan ook goede bekenden van ons. Voor hen zijn we een toegankelijke partner, gewend met vertrouwelijke informatie om te gaan en die als geen ander weet welke dreiging zich kan voordoen.

Voor ons is het onderkennen van de digitale dreiging topprioriteit. Want we willen de veiligheid van Nederlandse belangen hier of in het buitenland, onze informatiesystemen en onze economische belangen zeker stellen.

De menselijke factor speelt hierbij ook een grote rol. Alertheid van het personeel kan moedwillige schade aan het bedrijf en diens imago helpen voorkomen. Aan die alertheid gaat bewustwording vooraf. En voor die *awareness*, zo noemen we dat, kunt u terecht bij de AIVD. Dan plaatsen we tegelijk de dreiging in perspectief. Veiligheid vergt investeren, zowel in menskracht als in geld. En een gedegen afweging. Ik ben ervan overtuigd dat dat loont.

Het is mijn ervaring dat een gedegen voorbereiding het halve werk is op het vlak van veiligheid en crisisbeheersing. Dat wil niet zeggen dat er zich, ook in het vitale domein van onze maatschappij, geen crisis meer zal voordoen. Een goede voorbereiding is een belangrijke steun bij de beheersing van een moeilijke en mogelijk gevaarlijke situatie. Het geeft de rust die nodig is en de overtuiging om besluiten te durven nemen. Een dergelijke voorbereiding vraagt bekendheid met elkaars mogelijkheden en verwachtingen. Door middel van bezoeken, presentaties, briefings en op andere manieren maakt de AIVD zich daarom, ook als er geen sprake is van een directe dreiging, sterk voor een goede wisselwerking met vitale bedrijven.

Rob Bertholee
Directeur-Generaal Algemene Inlichtingen en Veiligheidsdienst

VITAAL PROCES SCHEEPVAARTAFWIKKELING IN NIEUW DAGLICHT

Port Call Optimization zorgt voor efficiencyslag

De Rotterdamse haven is van wezenlijk belang voor de Nederlandse economie. De afwikkeling van de scheepvaart is essentieel voor de haven en derhalve ook van belang voor de Nederlandse economie. Met andere woorden: het is een vitaal proces. Met Port Call Optimization maakt het Havenbedrijf een nieuwe efficiencyslag.

René de Vries
Havenmeester, Havenbedrijf Rotterdam

De afwikkeling van de scheepvaart is een gedeelde activiteit.
De *verkeersbegeleiding* voorziet de scheepvaart van relevante informatie en adviezen vanuit de helicopterview die de radarbeelden ons verschaffen.
De *loodsen* stappen daadwerkelijk aan boord van schepen om de kapitein te adviseren over de veilige navigatie naar de ligplaats in de haven. De loods is bij uitstek de expert met de lokale kennis die de kapitein zelf dikwijls ontbeert.
De *slepers* helpen een handje bij het manoeuvreren in nauw vaarwater en bij lastige bochten.
De *roeiers* maken de schepen vast.
Allemaal prachtig werk!

De *havenmeester* speelt ook een belangrijke rol in de coördinatie van een havenbezoek waarbij zaken als verkeersplanning, input voor de logistieke planning, het informeren en mobiliseren van dienstverleners en toeleveranciers, scheepsagenten en overheden allemaal iets met het schip willen. Zaken doen, lading controleren, reparaties uitvoeren … noem maar op. Het Havencoördinatie centrum is het

Havencoördinatiecentrum Rotterdam

Incidentbestrijdingsvaartuig voor de Pioneering Spirit, het grootste schip ter wereld

epicentrum van de scheepsbezoeken waar alle informatie samen komt en alle vragen gesteld worden. Loodsen en havenmeester werken ook hier samen en bij incidenten wordt vanuit datzelfde centrum de crisisbeheersing georganiseerd met de veiligheids-driehoek en alle hulpdiensten. De afwikkeling van de scheepvaart gaat dus veel verder dan alleen de verkeersbegeleiding. Alle bezoeken moeten veilig, vlot, schoon en beveiligd (security) afgehandeld worden. Het belang van de haven is (als vier poten onder een tafel) aan deze vier randvoorwaarden gebonden: vlot, veilig, beveiligd en schoon. Dat biedt de haven de legitimiteit te blijven groeien en te blijven acteren als motor van de Nederlandse economie. *A licence to grow*.

Momenteel gaat veel aandacht uit naar het verbeteren van de informatie ten behoeve van de klanten en het optimaliseren van de gehele keten. Onder de noemer van *Port Call Optimization* worden data op elektronische platforms beschikbaar en zichtbaar gemaakt, wordt de informatie over de waterweg, ligplaatsen en dieptes op een uniforme wijze gedeeld met de klanten en wordt er geïnvesteerd in het verbeteren van de planningsinformatie. Al die activiteiten om de afhandeling van scheepsbezoeken te optimaliseren, vergen vooral veel van de samenwerkende partijen binnen de haven. Openheid, transparantie en het gevoel een gezamenlijk doel te hebben dat het eigen – korte termijn – belang overschrijdt, zijn de belangrijkste uitdagingen daarin. Technologie – en met name de verwerking en presentatie van big data – helpt daar ook bij. En de technologische ontwikkelingen gaan ongelofelijk hard, zonder dat iemand daar erg in heeft.

Het gehele vitale proces van scheepvaartafwikkeling zou wel eens in een nieuw daglicht kunnen komen te staan. De omgeving verandert. We worden geconfronteerd met schaalvergroting en de vraag is hoe lang die doorzet. Transportstromen veranderen. Olie maakt plaats voor gas. Raffinagecapaciteit in de haven wordt op termijn minder omdat er in Europa een overcapaciteit is en nieuwe investeringen die pas na decennia terugverdient. Wat vervoeren we over 20 jaar nog over zee? Printen we producten misschien wel zelf uit in 3D? We kennen nu al onbemande containerterminals waar de kranen op afstand bediend worden en de voertuigen volautomatisch over de terminal rijden. Er wordt al geëxperimenteerd met waterdrones en onbemande scheepvaart. Is het heel raar om te verwachten dat er straks onbemande binnenvaartschepen zijn die tussen terminals varen? Komen er ook zeeschepen die met de automatische piloot, met *sense and avoid* systemen op zee varen? Als een Boeing op de automatische piloot kan landen? Waarom niet? En zou het afmeren van schepen in 20 jaar tijd nog altijd met de hand en met trossen gebeuren of moet je eerder denken aan magnetische systemen? Als je de fantasie de vrije loop laat, dan betekent dat nogal wat voor de afhandeling van de scheepvaart. De informatie en adviezen die loodsen en verkeersbegeleiders nu geven, zijn straks misschien niet meer nodig of op een andere manier. De mensen achter het vitale proces zullen andere profielen hebben. De planning en afstemming zijn straks misschien grotendeels geautomatiseerd. Al is de helft er maar van waar, dan nog betekent het een andere invulling van het vitale proces scheepsafhandeling en andere kwetsbaarheid. Hoe verder de mens zich terugtrekt uit het proces, hoe meer aandacht er moet komen voor de beveiliging van informatie- en besturingssystemen. De bescherming tegen cyberaanvallen zal in de toekomst nog relevanter zijn dan ze vandaag de dag al is.

Maar, de toekomst is ongewis en er zullen veranderingen optreden die we nu nog niet voorzien. Het is daarom zaak om scherp te blijven kijken naar ontwikkelingen en de mogelijke risico's daarbij te beheersen en kansen te grijpen. En te blijven werken aan een slimme haven met een neus voor noviteiten en innovatiemogelijkheden.

Jaarlijks arriveren 29.000 zeeschepen en 90.000 binnenvaartschepen

Jaarlijks gebeuren ongeveer 15 significante ongevallen op ongeveer 800.000 scheepvaartbewegingen

Havengebied begint 57 kilometer voor de kust en eindigt 40 kilometer landinwaarts bij de Van Brienenoordbrug

Havenbedrijf Rotterdam is verantwoordelijk voor de bedrijvigheid in de haven en de divisie havenmeester zorgt voor de veiligheid en orde op het water

Afhankelijkheden en keteneffecten

Uitval of verstoring van vitale infrastructuren kan ernstige gevolgen hebben. De bescherming van Europese en nationale vitale infrastructuur vormt daarom een belangrijk onderdeel binnen het overheidsbeleid inzake Nationale Veiligheid. Onderlinge afhankelijkheden en gelijktijdig falen van vitale infrastructuren kan het risico versterken. Ter ondersteuning van de rijksoverheid, de veiligheidsregio's en de vitale sectoren voert TNO op nationaal en internationaal niveau onderzoek uit naar afhankelijkheden, mogelijke keteneffecten en beschermingsmaatregelen.

Marieke Klaver en Eric Luiijf
TNO

Geheel of gedeeltelijke uitval van bijvoorbeeld onze energievoorziening, drinkwater-, transport- en/of ICT-infrastructuren kan ernstige maatschappelijke gevolgen hebben. Een complicerende factor vormt de soms sterke mate van onderlinge afhankelijkheid. Hierdoor kunnen keteneffecten ontstaan waarin uitval van één vitaal product of dienst leidt tot grote verstoringen of zelfs algehele uitval van één of meer andere vitale diensten.
TNO onderzoekt de mate waarin deze vitale infrastructuur onderling afhankelijk is, welke mechanismen zorgen voor de, soms onverwachte, keteneffecten, hoe groot het risico daarvan is en hoe dit risico kan worden verkleind. Dit onderzoek maakt gebruik van methoden en technieken die veelal in internationale onderzoeksprojecten worden ontwikkeld. Voor de afhankelijkheidsanalyses (zie figuur) wordt ook gebruik gemaakt van een unieke database met gegevens over vitale infrastructuur-incidenten, keteneffecten en gevolgen.

RESULTATEN ANALYSES VAN INCIDENTEN

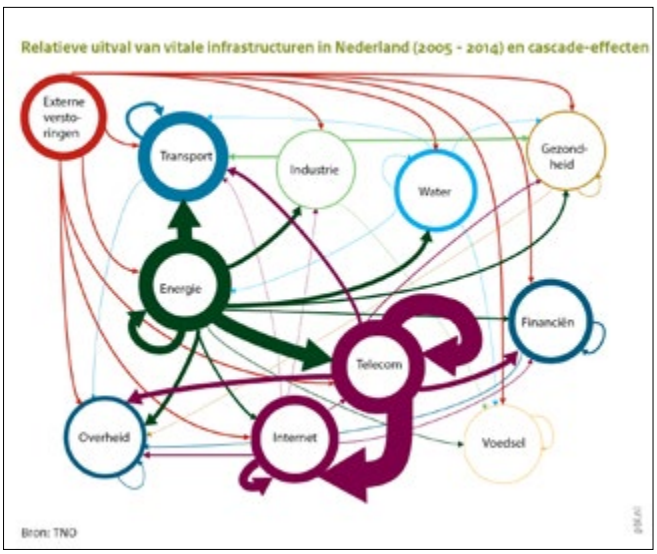
De analyses laten het volgende zien.

- Uitval in de elektriciteit- en ICT-sectoren leiden het vaakst tot keteneffecten in andere vitale infrastructuren.
- Vrijwel alle vitale infrastructuurorganisaties hebben een goed beeld van hun eigen vitale afhankelijkheden.
- Weinig vitale infrastructuurorganisaties hebben een goed beeld over hun vitale afnemers en de mate van de door hen getroffen mitigerende maatregelen tegen uitval.
- Hogere orde van afhankelijkheden en gemeenschappelijke kwetsbaarheden die meer objecten en infrastructuren gelijktijdig treffen, zijn als risicofactor in het algemeen slecht in risicoanalyses en crisisplannen verwerkt (zogenaamde *common mode failures*, bijvoorbeeld door een zware storm).
- Tijdens crisisomstandigheden kan het palet aan vitale afhankelijkheden aanzienlijk wijzigen ten opzichte van de normale bedrijfsvoering (bijvoorbeeld diesel, noodaggregaten en noodcommunicatie zijn ineens vitaal). Dergelijke afhankelijkheden zijn in het algemeen slecht bekend en daardoor nauwelijks in crisisplannen verwerkt. In die omstandigheden zijn veel partijen ook nog eens afhankelijk van dezelfde schaarse middelen; iets waar vooraf weinig rekening mee wordt gehouden.
- Na het teloor gaan van een vitale infrastructuur kan overwogen worden deze niet geheel opnieuw op te bouwen maar over te stappen op een geheel andere (modernere) infrastructuur.

Geen van de vitale infrastructuurorganisaties en betrokken overheidspartijen zijn afzonderlijk in staat om een goed beeld op te bouwen van de afhankelijkheden. Doordat individuele partijen niet in staat zijn om de gehele keten te overzien, zijn publiek-private samenwerking, informatie-uitwisseling en gezamenlijke (keten) analyses van groot belang.

TOEPASSING KENNIS OVER AFHANKELIJKHEDEN

Binnen de risicoanalyses die ten behoeve van de Strategie Nationale Veiligheid worden uitgevoerd, wordt de kennis over incidenten en keteneffecten toegepast bij het inschatten van de waarschijnlijkheid en de mogelijke impact. Daarnaast participeert Nederland in diverse EU-onderzoeksprojecten (zie kader). Door de steeds nauwere samenwerking met zowel de nationale overheid, de veiligheidsregio's en vitale bedrijven kan het ontwikkelde inzicht over de vitale afhankelijkheden maximaal worden benut in risicoanalyses en de planvorming voor crisisomstandigheden en herstel.



EU-onderzoeksprojecten vitale infrastructuur

- PREDICT: ontwikkelen van tools voor crisismanagement organisaties voor het analyseren van keteneffecten (www.predict-project.eu)
- CIPRNet: ontwikkelen virtueel Europees samenwerkingsnetwerk voor modellen en tools (www.ciprnet.eu)
  - NL inbreng: TNO en DELTARES; VenJ lid International Advisory Board
- INTACT: verhogen weerstand tegen extreem weer (www.intact-project.eu)
  - NL inbreng: TNO (consortiumleider), Deltares, Panteia
- DRIVER: innovatieve oplossingen voor crisis management en resilience (www.driver-project.eu)
  - NL inbreng: TNO, Ecorys, E-Semble, HKV Lijn in Water en Gemeente Den Haag (i.c. VR Haaglanden)

Domino congres brengt waterpartijen bij elkaar rond informatiemanagement

Rob Peters (IFV), Nico van Os (VR Zuid Holland Zuid), Gerke Spaling (VR Twente) en René Willems (TNO)

Op 20, 21 en 22 mei vond in Zwijndrecht het Dominocongres plaats. Domino adresseert de uitdaging van een "common operational picture" bij een groot overstromingsincident en de rol van informatiemanagement. Het IFV en de regio Zuid-Holland Zuid traden op als gastheer van een aantal geschakelde evenementen. Het geheel startte met een "VERA Masterclass informatie en risicomanagement" voor en door de veiligheidsregio's. Daarbij deelde landelijk CIO en Commandant Diemer Kransen het boek uit over twee jaar innovatie op het gebied van informatievoorziening bij die regio's. De door het Veiligheidsberaad goedgekeurde referentieachitectuur (VERA) is een kroon op dat digitale werk.

De daarop volgende discussie droeg er toe bij dat men nu met man en macht gaat werken aan de gemeenschappelijke definities van risico in het landelijk gegevensboek "firebrary". Tijdens de avond kwamen vijf Europese onderzoeksprojecten (Fortress, Driver, Predict, Sector en Casceff) aan bod in een "pitch". Dit was een opwarmer voor 18 workshops met de 160 deelnemers om de dialoog tussen praktijkmensen uit het veld, ontwikkelaars van modellen en ontwikkelaars van software goed te kunnen voeren.

Verbindend thema was het delen van de risicobeelden rond overstroming vanuit de rivieren, vitale infrastructuur en de bijdrage van de verschillende partijen voor het creëren van een gemeenschappelijk beeld. Dat gold ook voor bedrijven als Dupont of een partij als het Havenbedrijf. Gastheer Carlo Post leidde de dag in, samen met Arike Tomson van de Waterschappen en Christina Braliescu van de Europese Commissie (*Civil Protection Unit*). Buiten waren zes CoPi-bakken opgesteld, die met een veelheid aan digitale systemen met elkaar illustreerden dat we nog lang geen gedeeld beeld van de domino-effecten bij een overstroming kunnen hebben. Bovendien is de duiding van al die data een vraagstuk dat alleen opgelost kan worden wanneer betrokken partijen vooraf met elkaar in gesprek gaan. Nederland heeft een voortrekkersrol dankzij onze worsteling met LCMS, GMS en het aansluiten van andere systemen van bijvoorbeeld economische partijen als Schiphol of Rijkswaterstaat. De waterschappen zoeken intensief naar een gulden middenweg tussen "hun" systemen en zo'n netcentrische aansluiting. De CIO's van de regio's weten inmiddels wat de kracht is en wat de beperkingen zijn.

De workshops draaiden uit op een nogal organische ogende bijenkorf, waarbij groepjes debatterenden niet zelden op de knieën in de gang over kaarten gebogen hun verhitte betoog hielden. Het leek een chaos, maar de glim in de ogen van de deelnemers getuigde van een reeks zinvolle confrontaties.

European Project Officer Carla Gomez sloot de dag af met het stellige voornemen om het thema water en informatievoorziening terug te laten keren tijdens de Europese activiteiten in het kader van het EU-voorzitterschap van 2016. De veiligheidsregio's, het IFV en de waterpartijen pakken deze handschoen graag op en intussen zijn de eerste gesprekken over "crossborder"-oefeningen in 2016 met een informatiethema rond water al gevoerd. Deze formule van Domino om "het veld", "Brussel" en experts uit een aantal gelederen bij elkaar te brengen is goed bevallen. Volgend jaar in mei hopen we de ideeën en de ontwerpen van aanvullende systemen te kunnen toetsten in een "crossborder"-scenario rond onze rivieren. De Duitsers hebben al aangegeven dat ze graag met ons meedoen en dat is een goede zaak, want die rivieren komen deels daar vandaan.

Bescherming vitale infrastructuur en gevaarlijke stoffen - ontwikkelingen en toekomstperspectieven

Genserik Reniers
Hoogleraar Veiligheid Gevaarlijke Stoffen aan de TU Delft, U Antwerpen & KU Leuven

INLEIDING

Nederland is een dichtbevolkt land waar heel wat vitale infrastructuur aanwezig is. Het falen van vitale infrastructuur kan wegens de hoge bevolkingsdensiteit aanleiding geven tot grootschalige rampen. Uiteraard is het daarom belangrijk dat deze vitale infrastructuur optimaal wordt beschermd. “Optimaal” is natuurlijk relatief en hangt af van het standpunt van waaruit je het bekijkt. Abstractie makend van de vraag welke vitale infrastructuur beschermingsprioriteit heeft over andere vitale infrastructuur, kijken we in dit artikel enkel naar de vitale infrastructuur waarbij gevaarlijke stoffen zijn betrokken: de chemische industrie, de procesindustrie, de olie- en gasindustrie en de transporten van gevaarlijke stoffen. We gaan na wat de actuele denkpistes en de toekomstige (te verwachten) ontwikkelingen zijn op gebied van preventie en beheer, om deze vitale infrastructuur verder te beschermen tegen natuurrampen, veiligheid-gerelateerde catastrofes en security-gerelateerde geïnduceerde rampen (bijvoorbeeld ten gevolge van terrorisme).

VEILIGHEIDSPRINCIPES

De fundamentele veiligheidsprincipes zijn samen te vatten in vier kernpunten.

1. *Ontwerp:* aan veiligheid en security moet gedacht worden vanaf de allereerste fase, namelijk het ontwerp.
2. *Preventie:* één of meerdere barrières tussen gevaar en target(s) zijn nodig om de kans op een incident zo klein mogelijk te maken.
3. *Bescherming:* een adequate aanpak van de gevolgen is vereist (vóór ze zich manifesteren in een incident).
4. *Mitigatie:* als er toch iets misgaat en er zich dus een incident voordoet, moeten de gevolgen zoveel en zo snel mogelijk beperkt worden.

Vitale infrastructuur waarbij gevaarlijke stoffen zijn betrokken, vertaalt zich in praktijk als chemische bedrijvenparken met daartussen de nodige logistieke- en transportketens van chemische stoffen. Bekende voorbeelden van chemische bedrijvenparken in Nederland zijn die van de Haven van Rotterdam (bijvoorbeeld Moerdijk, Pernis, Botlek) en het park in Geleen (Chemelot). Als we de hierboven vermelde vier principes toepassen op veiligheid en security met betrekking tot chemische bedrijvenparken, komen we tot de volgende huidige en toekomstige ontwikkelingen en beheeraanpakken.

© *Shutterstock*

VEILIGHEIDSPRINCIPE 1: ONTWERP

Bedrijvenparken zijn een bestaand gegeven die niet meer ontworpen kunnen worden vanaf nul. Het ontwerp-veiligheidsprincipe dient zich bijgevolg te focussen op een wiskundig gefundeerde aanpak die aangeeft waar veiligheids- en security maatregelen op een ontwerp-gebaseerde intelligente manier dienen te worden genomen in de bedrijvenparken om deze veiliger te maken tegen toevallige rampen en tegen terroristische aanslagen. Door een bedrijvenpark te zien als één groot cluster van chemische installaties (ongeacht de individuele bedrijfsgrenzen) waartussen gevarenlinks bestaan (en ook deze links tussen elk paar installaties effectief in kaart te brengen), dan kan een bedrijvenpark worden voorgesteld als een wiskundig netwerk van gevarenlinks. Vervolgens kan worden bepaald waar de grootste gevaren bestaan in de netwerken en waar ontwerp-geba-

seerde maatregelen dienen te worden genomen zodat de gevolgen van rampen en aanslagen binnen bedrijvenparken optimaal kunnen worden beperkt. Om dit te realiseren dient een "Cluster Raad" te worden opgericht die op een hoger niveau dan individuele bedrijven informatie kan verzamelen en verwerken en – op basis van bedrijfsgeclusterde analyses – beslissingen kan nemen.

Op gebied van transporten van gevaarlijke goederen wordt gedacht aan een *secure lane* binnen Europa (onder andere met bewaakte parkings) waar transporteurs desgewenst gebruik van kunnen maken. Ook kan gedacht worden aan meer harmonisatie binnen Europa op gebied van risico-assessments voor transporten van gevaarlijke goederen en meer oog voor intermodale of a-modale transporten ter bevordering van veiligheid en security.

VEILIGHEIDSPRINCIPE 2: PREVENTIE

Op gebied van preventie met betrekking tot veiligheid wordt samenwerking tussen bedrijven binnen chemische bedrijvenparken steeds belangrijker in Europa. De Europese Seveso III Richtlijn die van kracht werd op 1 juni 2015 legt bijvoorbeeld meer nadruk op transparantie van bedrijven naar omwonenden toe en hecht ook meer belang aan informatie-uitwisseling tussen bedrijven. Bedrijven zelf beseffen ook steeds meer dat samenwerking op gebied van veiligheid en security tot win-win situaties kan leiden en werken daarom steeds meer met elkaar samen. Momenteel gebeurt de samenwerking nog steeds bijna uitsluitend operationeel en reactief (bijvoorbeeld uitwisseling van informatie over ongevallen), maar naar de toekomst toe kan zeker worden verwacht dat de samenwerking ook strategisch en proactief uitgebouwd zal worden en verder zal intensifiëren.

Op gebied van preventie met betrekking tot security, dus betreffende alle security-maatregelen binnen chemische bedrijven en bedrijvenparken, kan er nog een hele inhaalbeweging worden gemaakt. Momenteel is dit een sterk ondergewaardeerd domein binnen chemische bedrijven en bij chemische transporteurs. Daarom wordt aan universiteiten wereldwijd gewerkt aan meer kwantitatieve security risicoanalyses en verwacht kan worden dat er ook steeds meer hoogtechnologische oplossingen zullen worden gebruikt om hoogtechnologische dreigingen (zoals cybersecurity of mogelijke aanvallen met drones) adequater aan te kunnen pakken.

VEILIGHEIDSPRINCIPE 3: BESCHERMING

In Nederland spreekt men niet meer zozeer van een "risico-gebaseerde aanpak", dan wel van een "risico-gerichte aanpak". Het verschil tussen de twee begrippen wordt bepaald door het verschil tussen perceptie en realiteit. Een risico-gerichte aanpak gaat ervan uit dat nulrisico niet bestaat in realiteit en dat de bevolking dit ook beseft. Economische randvoorwaarden en ook morele aspecten moeten daarom worden meegenomen bij beslissingen rond beschermende maatregelen, naast de typische ongevalsscenario's met gevolgen en kansen. Tegelijk moeten bedrijven meer beseffen dat veiligheid en security op een continue manier leiden tot hypothetische baten en eigenlijk alternatieve vormen van "winst maken" zijn – net zoals innovatie en productiviteit dat zijn.

Het concept van inspectie en handhaving kan ook herdacht worden en er kan aan andere financieringsconcepten worden gedacht. Het principe van "de vervuiler betaalt" kan bijvoorbeeld toegepast worden op veiligheid. Er kan gedacht worden aan een systeem waarbij de eerste inspectie betaald wordt door de overheid en de noodzakelijke opvolgende inspecties bij de onveilige bedrijven gefinancierd worden door die bedrijven zelf (zoals in de UK).

Er kan bovendien ook gedacht worden aan inspectie en handhaving specifiek gericht op security in chemische bedrijven, hetgeen nu niet het geval is.

VEILIGHEIDSPRINCIPE 4: MITIGATIE

Mitigatie is het enige reactieve veiligheidsprincipe: het tracht de gevolgen van gebeurde ongevallen te beperken. Uiteraard bestaat er al heel wat op gebied van beteugeling in het kader van crisismanagement, maar ook hier kan nog veel meer worden samengewerkt tussen bedrijven. Voornamelijk in de cruciale korte tijdspanne vlak na de initiatie van een ongeval kan nog verder worden geoptimaliseerd in de beteugeling. Er kan een gezamenlijke bedrijvenparkmatrix voor crisismanagement worden ontwikkeld waar bedrijven vanaf het eerste moment perfect weten welke stappen te zetten op basis van ongevalsscenario's, zoals informatie-uitwisseling rond het ongeval, evacuatierichtlijnen, gebruik van schuilplaatsen van buurbedrijven en dergelijke. Ook potentiële escalerende ongevallen tussen bedrijven kunnen in de matrix worden opgenomen. Op die manier kan er veel sneller worden ingespeeld op een ongevalsscenario en kunnen de potentiële gevolgen veel sneller, en dus beter, worden beteugeld.

CONCLUSIES

Op gebied van veiligheid en security van vitale infrastructuur waarbij gevaarlijke stoffen zijn betrokken, zijn er verschillende wegen voorwaarts.
De *eerste* weg voorwaarts betreft een meer ontwerp-gebaseerde aanpak waarbij op een intelligente manier veiligheids- en security maatregelen worden getroffen, bijvoorbeeld vanuit een overkoepelende "Cluster Raad".
De *tweede* weg is die van de samenwerking tussen bedrijven in zogenaamde bedrijvenparken: op gebied van alle veiligheidsprincipes kan beter (meer proactief en strategisch) worden samengewerkt.
De *derde* weg is die van de maturiteit van security: bedrijven dienen security veel serieuzer te nemen en dienen veiligheid en security te beschouwen als een manier van winst maken.
De *laatste* weg is die van de inspectie en handhaving: ook security kan een belangrijk te handhaven domein worden in vitale infrastructuren waarbij gevaarlijke stoffen zijn betrokken.

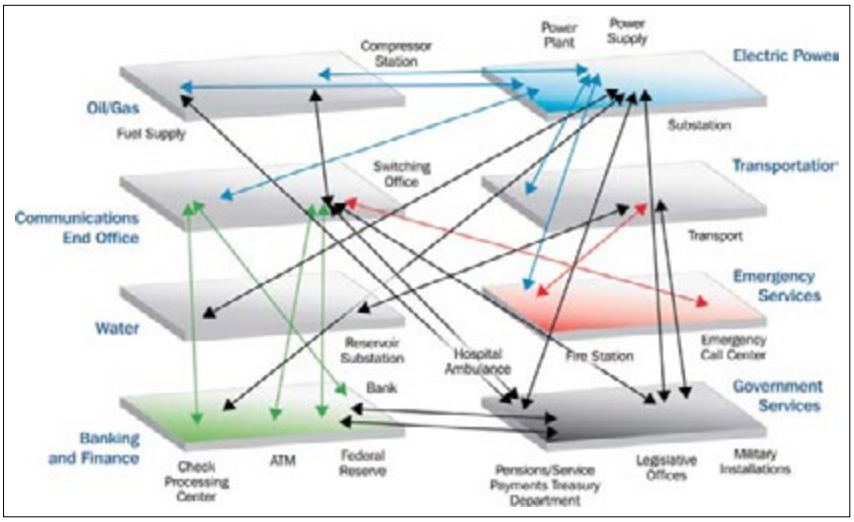
Hoe kwetsbaar is Nederland voor zonnestormen?

Dr. G. (Bert) H.J. van den Oord
Coördinerend specialistisch adviseur, KNMI

In de Nationale Risico Beoordeling 2011 is het uitvallen van satellieten ten gevolge van magnetische explosies op de Zon (zonnevlammen) als een mogelijk risico met ernstige consequenties voor de vitale sectoren geïdentificeerd. Sterke zonnevlammen sturen snelle deeltjes, hoogenergetische straling en soms grootschalige magnetische structuren met daarin materie (zogenaamde coronale massa-ejecties: CMEs) de ruimte in (vergelijk een Mount Everest die met 450 - 2000 km/s beweegt). De totale energie van een standaardvlam is ongeveer gelijk aan 67 miljoen atoombommen. De straling en snelle deeltjes bereiken ons in 8 minuten. De CMEs doen er uren tot dagen over en missen gelukkig vaak de aarde. De mensheid is altijd goed beschermd geweest tegen de effecten van zonnevlammen door de aardse ionosfeer, het magneetveld van de Aarde en de grote afstand tussen Zon en Aarde. Nu satellieten buiten deze beschermende lagen opereren, werkt deze bescherming niet meer. Ook de signalen van satellieten, zoals GPS en telecommunicatie, moeten door die ionosfeer en worden onbruikbaar als de ionosfeer door zonneactiviteit (*spaceweather*) wordt verstoord.

In 2013 is daarom in opdracht van IenM (en uitgevoerd door Cap Gemini) een Inventarisatie Kwetsbaarheden Uitval Satellietnavigatie (IKUS) gestart om de weerbaarheid van alle vitale sectoren tegen uitval van satellietnavigatie inzichtelijk te maken en zo nodig te vergroten. Deze inventarisatie, welke tot eind 2015 loopt, is van belang om maatschappelijke ontwrichting en grote economische impact bij uitval van satellietnavigatie te voorkomen. Tevens heeft IenM in 2015 aan het KNMI de opdracht gegeven tot een voorstudie voor een *spaceweather*-alarmeringsservice. Bij de start van de inventarisatie door het KNMI viel een aantal zaken op: de meeste West-Europese landen en VS, Canada, Brazilië, Japan, China en Zuid-Korea hebben al operationele waarschuwingsdiensten en er zijn internationale consortia als ISES (*International Space Environment Services*) die alertering-services verlenen. Daarnaast blijkt 2015 een zeer interessant jaar voor *spaceweather* te zijn. Het *Committee on Space Research* (COSPAR) was in de afrondende fase van een roadmap voor de toekomstige mondiale *spaceweather*-infrastructuur. Ook loopt er een herstructurering van de Internationale Astronomische Unie (IAU). Het KNMI is vanaf dit jaar vertegenwoordigd in twee commissies van de IAU die bepalend zijn voor *spaceweather*-onderzoek. Tenslotte heeft de Wereld Meteorologische Organisatie (WMO) – waarin het KNMI Nederland vertegenwoordigt – *spaceweather* tot een prioriteit gemaakt en het idee is dat de mondiale meteorologische infrastructuur gebruikt gaat worden voor uitwisseling van *spaceweather*-waarschuwingsproducten. Deze laatste ontwikkeling wordt sterk gedreven door de *International Civil Aviation Organization* (ICAO) die behoefte heeft aan één geautoriseerde waarschuwingsservice voor de luchtvaart. Bij Defensie experimenteert de *Joint Meteorology Group* (JMG) in Woensdrecht met *spaceweather*-producten. Vanwege de traditioneel sterke samenwerking tussen KNMI en JMG worden voor de voorstudie kennis en ervaringen gedeeld.

Waarom zijn deze ontwikkelingen bij COSPAR, IAU, ISES en WMO zo belangrijk? De infrastructuur voor *spaceweather*-observaties kost ettelijke miljarden Euro's: er zijn talloze satellieten, radiotelescopen en optische telescopen die de Zon monitoren en op veel plaatsen op aarde wordt het gedrag van de ionosfeer en het aardmagnetisch veld gemeten in observatoria. Tenslotte zijn er vele modellen, vergelijkbaar met weermodellen, die het magneetveld op de Zon, de interplanetaire ruimte, de aardse ionosfeer en het aardmagneetveld modelleren ten behoeve van verwachtingen en alerts. De budgetten voor deze infrastructuur komen voornamelijk uit onderzoeksprogramma's waarvoor organisaties als COSPAR en IAU richtingbepalend zijn. Daarom is het van belang in die gremia vertegenwoordigd te zijn. Veel *spaceweather*-waarschuwingsproducten worden uiteindelijk beschikbaar gesteld via de *spaceweather*-service van de *National Oceanic and Atmospheric Administration* (NOAA).



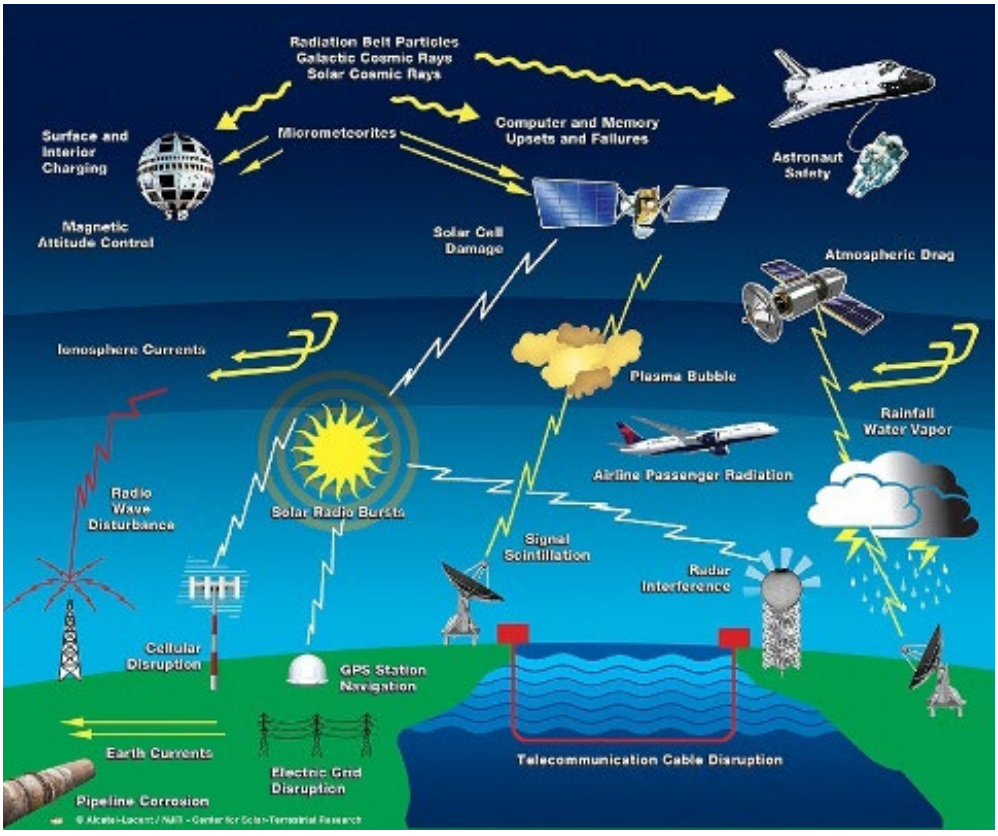
Keteneffecten elektriciteitsvoorziening space weather (VS)

Deze producten vormen de grondstoffen voor de meeste andere waarschuwingsservices die momenteel actief zijn. Deze producten zeggen iets over het activiteitsniveau van de Zon en ionosfeer maar niets over effecten op sectoren!

Indien er al zoveel informatie beschikbaar is, waarom in Nederland dan nog een nationale service inrichten? Dat heeft te maken met het gegeven dat het effect op de vitale infrastructuur per land aanzienlijk verschilt! Een simpel voorbeeld is het lopende experiment waarbij JMG vanuit Woensdrecht een waarschuwingsproduct voor telecommunicatie en GPS-verstoringen levert aan onze troepen in Mali en voor oefeningen in de Oostzee. Voor telecommunicatie is dit product door de geografische ligging van Nederland minder belangrijk maar wel weer voor de BES-eilanden. Van de andere kant lijken effecten van GPS-verstoringen voor Nederland steeds belangrijker te worden door het groeiend aantal toepassingen (smart cars, smart agriculture, etc.). Ook verandert de gevoeligheid voor zonneactiviteit van elektriciteits- en communicatienetwerken door schaalvergroting op Europees niveau. Effecten op radars voor scheepvaartafhandeling dienen verder te worden onderzocht. De uitdaging ligt in het vertalen van de beschikbare *spaceweather*-producten naar specifieke waarschuwingen voor ieder van de vitale sectoren.

Uitgaande van de aanname dat het leveren van waarschuwingsproducten geen onoverkomelijke problemen oplevert, blijkt er een veel lastiger probleem zich voor te doen bij het opzetten van een service en dat betreft het opzetten van een dialoog met vitale sectoren. De activiteitscyclus van de Zon heeft een periode van 11 jaar. Per cyclus van 11 jaar zijn er 3 tot 8 dagen van ernstige tot zeer ernstige aardmagnetische verstoringen, energetische deeltjes en telecommunicatieproblemen. Als we risico beschrijven als kans maal impact dan hebben we bij *spaceweather* te maken met een kleine kans maar met een enorme impact. Voor gebeurtenissen met een kleine kans blijkt het moeilijk om bewustzijn te creëren. De effecten op bijvoorbeeld de elektriciteitsvoorziening kunnen zeer groot zijn maar de kans is klein. Anderzijds is het aantal kleine GPS-verstoringen veel groter (duizenden per cyclus) maar deze hebben een kleinere impact totdat we naar nieuwe technologieën overstappen zoals zelfsturende auto's. Wat dat betreft heeft het afgeven van een weeralarm door het KNMI een directer effect omdat het aansluit bij het dagelijks ervaren van het weer. Ook blijkt dat bij de nationale risicoanalyse vooral is gekeken naar het effect satellieten en hun functie (bijvoorbeeld GPS) terwijl in Nederland grote ketenafhankelijkheden kunnen optreden indien bijvoorbeeld door een CME-verstoring het elektriciteitsnetwerk of het internet uitvalt. Dit heeft direct een effect op vele sectoren. Het is daarom belangrijk om in 2015 samen met de vitale sectoren de ketenafhankelijkheden in kaart te brengen. Het is interessant om op te merken dat in de herijkte lijst voor de vitale infrastructuur (brief minister Van der Steur aan Tweede Kamer) alle processen gevoelig zijn voor *spaceweather*. Indien niet direct, dan toch via ketenafhankelijkheden! Daarmee kan *spaceweather* cascade-effecten veroorzaken die vergelijkbaar zijn met uitval van elektriciteitsvoorziening door andere oorzaken. Het KNMI gaat de komende periode verder met die dialoog met de sectoren (netwerkbeheer, veiligheidsregio's, DCCs, havenbedrijven, telecomsector, financiële sector, internet en dataverkeer etc.) en vooral met het geven van lezingen om het bewustzijn te vergroten. Ook zullen modellen voor ketenafhankelijkheden vertaald worden naar de Nederlandse situatie en zal de samenwerking met de *Joint Meteo Group* van Defensie worden uitgebouwd.

Ten slotte zal een goede inbedding van de KNMI *spaceweather*-service binnen het informatiesysteem van de WMO niet alleen resulteren in het beschikbaar komen van goede producten maar ook in internationale kennisuitwisseling voor dit complexe en belangrijke onderwerp dat de gehele Aarde betreft maar zeer specifieke lokale/nationale risico's voor vitale sectoren introduceert.



Artist impression effecten op sectoren

Luchtvaart als vitale sector

Medio 2013 werd door de NCTV aangevangen met het Traject Herijking Vitaal. In het kort hield deze exercitie een revisie in van de bestaande uitgangspunten van het beleid voor Vitale Infrastructuur in Nederland, alsmede wijziging van relevante parameters om het beleid van een algehele update te voorzien. Deze "update" hing al enige tijd in de lucht en als belangrijk onderdeel hiervan was Luchtvaart een van de sectoren die nader onder de loep werd genomen.

Marc van Oudheusden
Directie Luchtvaart, Ministerie van Infrastructuur en Milieu

De herziening is belangrijk en wordt voor alle vitale sectoren op een min of meer gelijke wijze ingericht. Betrokkenheid van de sector en andere primaire stakeholders bepalen in belangrijke mate de luchtvaart-specifieke invulling van de generieke criteria voor vitaliteitsbepaling. Het inrichten van noodzakelijke vervolgstappen vormen daarbij de kern.

Voor luchtvaart is dit initiatief van belang en de wisselwerking en afstemming met de NCTV wordt daarbij als bijzonder positief en ondersteunend ervaren. De sector Luchtvaart wordt in het kader van crisisbeheersing en continuïteitvraagstukken over het algemeen ingedeeld in drie subdelen, namelijk luchtvaartmaatschappijen, luchthavens, de luchtverkeersdienstverlening. En dan uiteraard de bestuurlijke component daarbij. In de "oude" systematiek was gekozen voor de gerichte onderverdeling in vitale en niet-vitale onderdelen binnen de luchtvaartsector. Deze onderverdeling bleek echter niet meer op zijn plaats. In de loop van de jaren is de ketenbenadering ook binnen de luchtvaart in betekenis toegenomen. Alle producten en diensten van alle separate onderdelen zijn feitelijk in het totale proces van diensten aan elkaar verbonden. Dit betekent dat de onderverdeling zoals een jaar of tien geleden vastgesteld, inmiddels als achterhaald kan worden bestempeld.

Deze onderlinge afhankelijkheid en verbondenheid van alle onderdelen binnen de luchtvaart worden met name ook bij het dossier cybersecurity nadrukkelijk gevoeld. Met name richting de toekomst zullen alle systemen en diensten nog veel meer met elkaar verweven raken. Daarmee wordt de kwetsbaarheid van de "zwakste" schakel in het totale systeem, met name als het gaat om verstoring van de continuïteit, steeds bepalender.

Een andere ontwikkeling die binnen de luchtvaart grote sporen heeft nagelaten heeft betrekking op het zich voordoen van grote crisis scenario's. De aswolk uit 2010 en 2011 heeft daarbij als voorbeeld een onuitwisbare indruk gemaakt. We spreken in dit verband over scenario's als grote weersveranderingen, langdurige stakingen, (dreiging van) terroristische aanslagen en zonnestormen. Het zijn allemaal voorbeelden van crisissituaties die de continuïteit van de luchtvaartsector op nationaal en ook Europees niveau ernstig kunnen bedreigen. Het luchtvaartsysteem is inmiddels mondiaal verbonden, waardoor crises in regio's ver buiten Europa toch ook hier grote gevolgen kunnen hebben. De tsunami in Japan, de gespannen situatie in de Oekraïne en Electra-uitval in de VS zorgden voor hoofdbrekens en vraagtekens, ver voorbij de reguliere continuïteitsvraagstukken.

In het licht van nadere invulling van deze crisisscenario's en de noodzakelijke mitigerende maatregelen is het uiteraard van groot belang dat duidelijk inzicht bestaat in de kritische vitale sectoren en processen in ons land in algemene zin en natuurlijk ook luchtvaart specifiek.

Op basis van de analyse, waarin alle stakeholders participeerden, is inmiddels komen vast te staan dat de Luchtvaart in Nederland onder "Vitaal B" valt, net als de haven Rotterdam en enkele andere infrastructurele onderdelen. Inmiddels is de vaststelling van deze categorisering een feit en is dit jaar begonnen met de nadere implementatie en invulling van de zogenaamde "road-map", een soort overzicht waarin nader wordt bepaald welke (organisatorische) gevolgen een en ander in praktische zin voor de specifieke vitale onderdelen zou kunnen hebben. Dit traject is inmiddels ook gemeld aan het parlement en wordt verder afgewikkeld onder auspiciën van de Stuurgroep Nationale Veiligheid.

Aanpak overstromingsrisico's nationale vitale en kwetsbare functies

In het Deltaprogramma is al geruime tijd extra aandacht voor de overstromingsrisico's van zogeheten vitale en kwetsbare functies. In dit artikel wordt kort geschetst voor welke aanpak er is gekozen. Achtereenvolgens wordt beschreven waarom een speciale aanpak voor vitale en kwetsbare functies nodig is, om welke functies het eigenlijk gaat en wat de aanpak is voor de komende jaren. Daarbij wordt ingegaan op de verantwoordelijkheidsverdeling en op de eerste resultaten van de aanpak.

Jasper Groos
Rijkswaterstaat, Ministerie van Infrastructuur en Milieu

De aanpak van vitale en kwetsbare functies begint met de Deltabeslissing ruimtelijke adaptatie (onderdeel van het Deltaprogramma 2015). In deze Deltabeslissing wordt onder meer vastgesteld dat "het Rijk er voor zorgt dat nationale vitale en kwetsbare functies uiterlijk in 2050 beter bestand zijn tegen overstromingen". Daarbij wordt een aanpak gekozen die uiterlijk in 2020 tot beleid of regelgeving leidt en waarbij een stappenplan wordt gebruikt van "weten, willen en werken".

WAAROM EEN AANPAK?

De extra aandacht voor vitale en kwetsbare functies in het Deltaprogramma heeft een drietal goede redenen. Door een *overstroming* kunnen essentiële voorzieningen van een samenleving uitvallen, zoals de energievoorziening, telecommunicatie en drinkwaterlevering. Ook kunnen er *gevaarlijke stoffen vrijkomen* uit nucleaire installaties, chemische bedrijven of uit het rioolsysteem, met alle risico's van dien voor mens en milieu. Ten slotte ontstaat er grote *economische schade* als gebieden door een overstroming tijdelijk onbewoonbaar zijn of als belangrijke bedrijven lange tijd stil komen te liggen door een overstroming.

OVER WELKE FUNCTIES GAAT HET?

De aanpak van de overstromingsrisico's van vitale en kwetsbare functies gaat deels over de zogeheten "vitale functies" waarover in april een voortgangsbrief over nationale veiligheid aan de Tweede Kamer is gestuurd. Het gaat dan over energie (elektriciteit, gas, olie) en telecom, over bedrijven in de waterketen (drinkwater en afvalwater) en over chemische bedrijven en kerncentrales. Maar de aanpak gaat ook over andere functies die kwetsbaar zijn voor overstromingen, zoals onze hoofdwegen, gemalen, ziekenhuizen of bedrijven die werken met infectieuze stoffen.

Elektriciteitshuisje Ooijpolder © Martien Versteegh, Donkigotte

AANPAK: WETEN, WILLEN, WERKEN

In het Deltaprogramma van 2015 is een aanpak gekozen om de water robuuste inrichting in 2050 te bereiken van vitale en kwetsbare functies. Deze aanpak bestaat uit een stappenplan van "weten", "willen" en "werken".

1. *Weten*: de verantwoordelijke ministeries brengen in de periode 2015-2016 samen met de sectoren de kwetsbaarheden en risico's in beeld.
2. *Willen*: er wordt in de jaren tot 2020 voor iedere functie een strategie bepaald: een ambitie plus de concrete stappen om deze te halen. Voor 2020 is dus ook beleid (en eventueel regelgeving) en toezicht gereed.
3. *Werken*: voor 2050 zijn de benodigde maatregelen genomen, gekoppeld aan reeds geplande investeringsbeslissingen binnen de sector.

VERANTWOORDELIJKHEIDSVERDELING

Verschillende ministeries zijn verantwoordelijk voor de afgesproken aanpak. Het ministerie van Economische Zaken gaat bijvoorbeeld over de aanpak van energie en telecom. Het ministerie van VWS over ziekenhuizen en infectieuze stoffen.Het ministerie van Infrastructuur en Milieu, dat zelf ook verantwoordelijk is voor een aantal functies, coördineert de aanpak de komende jaren. Belangrijk daarbij is de afbakening van de verantwoordelijkheden tussen Rijk en regio: sommige functies vragen een sectorale aanpak op Rijksniveau terwijl andere functies beter water robuust kunnen worden gemaakt als onderdeel van een (vaak meer lokale) integrale gebiedsontwikkeling.

EERSTE RESULTATEN VAN DE AANPAK

Binnen veel functies is men momenteel druk bezig met de stap "weten": het krijgen van inzicht in de aard en omvang van de risico's die een overstroming met zich meebrengt. Sommige functies zijn al verder en een enkele functie is zelfs al klaar met de aanpak. In het Deltaprogramma 2016, dat met Prinsjesdag 2015 wordt gepresenteerd, zal de voortgang van de aanpak worden beschreven.

Bescherming vitale infrastructuur in Duitsland - quo vadis?[1]

Dr. Monika John-Koch
Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

MEER VRAGEN DAN ANTWOORDEN?

Ruim tien jaar geleden werd de basis gelegd voor een strategisch-conceptionele en institutioneel-organisatorische oplossing voor de bescherming van vitale infrastructuren (*Schutz KRITIS*). In 2009 werd in Duitsland de Nationale strategie ter bescherming van vitale infrastructuren vastgesteld en geïntegreerd in de wetgeving. Bond en deelstaten kwamen tot een gezamenlijke definitie en indeling in negen sectoren; er werden solide samenwerkingsverbanden opgezet tussen staat en bedrijfsleven. Analyses en aanbevelingen vormen min of meer concrete uitkomsten van de jarenlange inspanningen ter bescherming van vitale infrastructuren.
Maar naarmate de bescherming van vitale infrastructuren pregnanter wordt of – zo u wilt – populairder, hoe meer regelingen of strategisch-planologische besluitvorming er nodig zijn, die op hun beurt weer meer vragen doen rijzen waarop tot dusver nog geen bevredigende antwoorden zijn gevonden. Welke infrastructuren zijn er nu echt vitaal? Levert de focus op inrichtingen en organisaties die onder de definitie vallen wezenlijke aspecten van vitale infrastructuren op? Valt bescherming van vitale infrastructuren überhaupt te realiseren?

CONFLICTERENDE BELANGEN

In de KRITIS-Strategie worden het doel en de politiek-strategische uitgangspunten van de Bond samengevat, worden aspecten qua methodiek en procedures belicht en actoren voor de bescherming van vitaleinfrastructuur aangesproken. Bij herhaling wordt de gezamenlijke verantwoordelijkheid van overheid en bedrijfsleven benadrukt en worden alle verantwoordelijken opgeroepen samen te werken. Maar aan deze oproep valt vanwege de uiteenlopende structuren, procedures en belangen en de verschillende opvattingen over optreden en besluitvorming minder eenvoudig te voldoen dan op het eerste gezicht lijkt.

SAMENWERKING TUSSEN DE AUTORITEITEN

De autoriteiten beschouwen de bescherming van de vitale infrastructuur doorgaans als onderdeel van de sectorspecifieke beveiliging. Daarom ligt de verantwoordelijkheid in het kader van hun mandaat bij de ministeries voor het treffen van regelingen ter waarborging van de bescherming van "hun" infrastructuren. Voor een sectoroverstijgend thema als de bescherming van vitale infrastructuren dienen er verschillende belangen tegen elkaar te worden afgewogen. Economische aspecten verdragen zich nu eenmaal niet altijd met milieuoverwegingen of kunnen ten koste gaan van de veiligheid. Er is coördinatie nodig om strategieën en programma's op elkaar af te stemmen, synergieën te benutten en te kunnen waarborgen dat er op federaal niveau uniform gehandeld wordt. Het *Bundesministerium des Innern*/ministerie van Binnenlandse Zaken (BMI) coördineert de activiteiten in het kader van KRITIS namens de federale overheid.

Voor de contacten tussen Bond en deelstaten fungeert BMI als aanspreekpartner voor de overkoepelende strategische aspecten. Specifiek sectorgebonden kwesties worden afgestemd tussen de bevoegde Bonds- en deelstaatministeries. Binnen de "Arbeitsgruppe der Koordinierungsstelle Kritische Infrastrukturen" (AG KOST KRITIS) wisselen Bond en deelstaten informatie uit en worden onderzoeken en onderzoeksresultaten, methodes en aanbevelingen gepresenteerd en gezamenlijke standpunten uitgewerkt.

Zo is er een institutioneel kader gecreëerd voor Schutz KRITIS. In hoeverre er daadwerkelijk belangen worden afgewogen en strategieën en maatregelen worden afgestemd hangt natuurlijk af van de mogelijkheden en bereidwilligheid over ministeriële bevoegdheden en jurisdicties heen te plannen en te beslissen.

SAMENWERKING MET BEHEERDERS

Een groot deel van de verantwoordelijkheid voor de bescherming van vitale infrastructuren ligt natuurlijk ook bij de beheerders ervan. Dit blijkt ook uit de KRITIS-Strategie waarin de nadruk wordt gelegd op de gezamenlijke verantwoordelijkheid van staat en particuliere partijen voor de veiligheid, betrouwbaarheid en beschikbaarheid van vitale infrastructuren.

Deze gedeelde verantwoordelijkheid blijkt ook uit de opzet en uitbreiding van publiek-private partnerschappen teneinde sectoroverstijgende concepten en beschermende maatregelen te ontwikkelen, sectorspecifieke oplossingen uit te werken of afzonderlijke kwesties te behandelen, zoals IT-beveiliging. Hierbij is op federaal niveau uitdrukkelijk een rol weggelegd voor UP KRITIS (www.upkritis.de). Maar de mogelijkheden van partnerschappen stuiten op hun grenzen wanneer men er niet in slaagt een gezamenlijk standpunt inzake Schutz KRITIS uit te werken. Wanneer het streven naar maximale winst van ondernemers bijvoorbeeld niet te verenigen valt met staatsbelangen (bijvoorbeeld veiligheid) of -taken (bijvoorbeeld bescherming van de bevolking), dienen de partijen

[1] Dit artikel is een bewerking van een bijdrage in "*Bevolkerungsschutz* 4/2014 (www.bunde.de); daar ook verdere bronverwijzingen.

tot een vergelijk te komen dat recht doet aan hun beider belangen en samenwerking - hetgeen bij tijd en wijle moeizaam verloopt.

METHODIEK

Bij de activiteiten rond Schutz KRITIS rijzen steeds meer uitdagingen en kwesties rond de methodiek die deels de uitgangspunten voor Schutz KRITIS betreffen en mogelijk zullen leiden tot een andere manier van denken.

IDENTIFICATIE VAN VITALE INFRASTRUCTUREN

Wat abstract onder vitale infrastructuren verstaan moet worden, blijkt uit de volgende definitie: "Organisaties of voorzieningen die van groot belang zijn voor de gemeenschap en bij uitval of beschadiging langdurig kunnen leiden tot problemen, ernstige verstoring van de publieke veiligheid of andere dramatische gevolgen." Niet duidelijk is echter welke systemen en voorzieningen in concreto zo belangrijk zijn dat ze bijzondere bescherming behoeven. Het bankwezen biedt weliswaar een paar aanknopingspunten qua systeemrelevantie *(too big to fail)*, maar vragen vanuit de gemeenschap of schakelstation A, transformatorstation B, spoortracé Y of ziekenhuis Z of zij van vitaal belang worden geacht, kunnen er niet mee beantwoord worden.
Ook vanuit politiek en juridisch oogpunt is er behoefte aan duidelijkheid. Het wetsontwerp voor IT-beveiliging voorziet onder meer in beschermingsmaatregelen en een meldplicht voor beheerders van vitale infrastructuren. Om de reikwijdte concreet, toereikend en eenduidig vast te stellen dienen criteria te worden vastgelegd voor de identificatie van vitale infrastructuren die toepasbaar moeten zijn op alle sectoren en bestuurlijke niveaus.

Er wordt al geruime tijd gewerkt aan geschikte methoden en er zijn al enkele concepten, maar behalve de toetsing in de praktijk moeten ook de nodige procedures voor de politieke en juridische goedkeuring worden doorlopen.

INSTALLATIE OF SYSTEEM?

Inmiddels zijn er voor Schutz KRITIS afzonderlijke sectoren en branches en systemen onderzocht, zijn er per branche specifieke risicoanalyses verricht en portfolio's met maatregelen uitgewerkt. De vraag rijst echter of de focus op organisaties, voorzieningen en installaties wel de wezenlijke aspecten voor de bescherming van vitale infrastructuur oplevert. Is de oriëntatie op sectoren en branches leidend of moeten juist de vitale diensten centraal staan? Zou het – om de bevolking te kunnen blijven voorzien van goederen en diensten – niet moeten draaien om het systeem als zodanig? Vormen de netwerken, distributiepunten of knooppunten niet eerder vitale invalshoeken?

Juist vanwege de afhankelijkheden, interdependenties en mogelijke cascade-effecten levert een systeemgerichte invalshoek duidelijke grenzen op bij sectoroverstijgende analyses en dat geldt eveneens voor de ontwikkeling van noodconcepten.
De EU heeft hierop gereageerd met het voornemen het Europese programma ter bescherming van vitale infrastructuren (EPCIP) sterker toe te spitsen op systemen en diensten en sector overstijgende thema's op de voorgrond te plaatsen. Dit zal ook op nationaal niveau een grotere rol moeten gaan spelen.

© Dieter Schütz (pixelio.de)

BESCHERMING OF RESILIENCE?

Tot dusver hielden de autoriteiten, het bedrijfsleven en de wetenschap zich vooral bezig met kwesties op het gebied van de *bescherming* van vitale infrastructuren. Omdat steeds meer systemen in netwerken worden geïntegreerd of nieuwe bedreigingen vanuit cyberspace opdoemen rijst de vraag of het concept "Schutz" de lading van KRITIS nog wel dekt. Bescherming impliceert immers dat iets of iemand wordt behoed tegen een gevaar, afgeschermd wordt of dat het gevaar kan worden vermeden. Maar bescherming in deze zin is hier nauwelijks haalbaar, aangezien permanente bewaking van in netwerken geïntegreerde infrastructuren net zo moeilijk te realiseren valt als de volledige afscherming van communicatie-infrastructuren. Bij IT-infrastructuur ligt dit nog moeilijker, want die kan niet worden afgeschermd zonder aan functionaliteit in te boeten. Bovendien veranderen de bedreigingen voortdurend. Hoe kunnen informatie-infrastructuren betrouwbaar tegen aanvallen worden beschermd, wanneer de gehanteerde middelen, vectoren en doelen onbekend zijn? Vooral bij cyberrisico's wordt de problematiek omtrent "Schutz" duidelijk. Maatregelen kunnen alleen effectief zijn wanneer de gevaren bekend zijn, er prognoses kunnen worden gemaakt en snelle respons mogelijk is. Statische concepten hebben slechts beperkt nut in een dynamische, veranderlijke omgeving.

Naast het concept Schutz voor vitale infrastructuur is dan ook *resilience* nodig: het vermogen met allerlei storingen *om te gaan*, dat wil zeggen die te kunnen opvangen, verhelpen of aanpassingen door te voeren. Ook dit dient te worden meegenomen voor de toekomst.

CONCLUSIES

Al met al is er al veel bereikt wat betreft de bescherming van vitale infrastructuren als sectoroverstijgende taak voor de binnenlandse veiligheid. Er zijn echter nog een aantal organisatorische uitdagingen voor de samenwerking tussen partners met uiteenlopende belangen en eisen, alsmede kwesties omtrent methodes die logischerwijze rijzen bij intensievere beschouwing van vitale infrastructuren en die een gezamenlijke oplossing behoeven.

De internationale stand van zaken in de bescherming van vitale infrastructuur

Erwin van der Zwan en Marcel Spit
Adviescentrum BVI

Het Adviescentrum Bescherming Vitale Infrastructuur heeft voor de NCTV ter ondersteuning van de herijking van vitale infrastructuur een verkennende literatuurstudie uitgevoerd naar de stand van zaken ten aanzien van de bescherming van vitale infrastructuur (*Critical National Infrastructure*, CNI) in de Verenigde Staten, Canada, Australië, het Verenigd Koninkrijk en Denemarken. Het doel was om eventuele aanbevelingen of acties te identificeren die ook voor Nederland relevant kunnen zijn. Daarbij is ingezoomd op strategische aspecten en de sectoren elektriciteit, olie, gas, nucleair, drinkwater, telecom en keren en beheren waterkwantiteit.

De **Verenigde Staten** hebben de aanpak met name vastgelegd in het *National Infrastructure Protection Plan* (NIPP) van het *Departement of Homeland Security* (DHS). Het NIPP legt de nadruk op het verbeteren van security en veerkracht, het managen van risico's en een integrale benadering. Samenwerking tussen private partijen en de overheid is voornamelijk vrijwillig. In 2013 zijn de verantwoordelijkheden en taken van overheidsorganisaties aangescherpt in de *Presidential Policy Directive PPD-21 Critical Infrastructure Security and Resilience* en *Executive Order (EO) 13636 Improving Critical Infrastructure Cybersecurity*. Een aanvullend voorstel voor de aanpak van cybersecurity, de *National Cybersecurity and Critical Infrastructure Protection Act of 2014*, is eveneens gepasseerd. Speerpunten zijn de ontwikkeling van een technologie-neutraal Cybersecurity Framework, het bevorderen van cybersecurity praktijken en een tijdige uitwisseling van dreigingsinformatie. Daarnaast wordt aandacht gevraagd voor het verbeteren van het inzicht ten aanzien van fysieke en cyber aspecten over het functioneren van CNI in de tijd en de trapsgewijze gevolgen van infrastructurele storingen (cascade-effecten). Aanvullend eist het ministerie van Defensie en de *General Service Administration* dat voor het gunnen van contracten cybersecurity-eisen worden geformaliseerd.

De *U.S. Government Accountability Office* roept het DHS op om consistent te handelen met het NIPP raamwerk en te focussen op vitale infrastructuur met de hoogste prioriteit. Daarbij moeten kwetsbaarheidsgegevens over CNI-middelen, systemen en netwerken consequent door DHS worden verzameld en beheerd om potentiële doublures en lacunes te identificeren, de voornaamste gebruikte tools en methoden te analyseren en om afgedekte aandachtsgebieden te bepalen. Ook wordt gevraagd om een methode te ontwikkelen (zoals een security- en kwetsbaarheidsvragenlijst) om de bijdrage van individuele projecten aan de verbetering van de veerkracht van CNI te meten.

De *Strengthening Domestic Nuclear Security Act (HR 5629)* en de *Critical Infrastructure Protection Act (HR. 3410)* keuren acties goed om CNI, met name de elektriciteitssector, beter te beschermen tegen een elektromagnetische puls. Binnen de watersector wordt opgeroepen om detectie, respons en herstelplannen verder te ontwikkelen, het publieke en politieke begrip voor uitvaleffecten te vergroten en een waarschuwingssysteem voor verontreiniging van drinkwater te ontwikkelen. Chemische bedrijven worden verplicht om maatregelen tegen terrorisme te treffen en om door DHS goedgekeurde Site Security Plannen te hebben (HR 4007). Waterkerende installaties worden verplicht om NERC CIP standaarden te implementeren.

Canada heeft een *Action Plan for Critical Infrastructure 2014-2017* en een *Action Plan 2010-2015 for Canada's Cyber Security Strategy* opgesteld. Het Action Plan legt hierbij nadruk op bescherming tegen terrorisme, cybersecurity, klimaatveranderingen en globalisering. Canada zet verder in op verhogen van de capaciteit voor het verzamelen en analyseren van informatie en het detecteren van cyberdreigingen. Daarbij wordt een Industrial Control System laboratoriumprogramma (*National Energy Infrastructure Test Center*) opgezet en worden de mogelijkheden van het Canadese Cyber Incident Response Centrum uitgebreid om ondersteuning te bieden buiten de Canadese overheid.

Australië beschrijft haar aanpak in de *Critical Infrastructure Resilience Strategy Supplement* en volgt daarbij voornamelijk een niet-regelgevende benadering. Australië richt zich op het ontwikkelen van sterke samenwerkingsverbanden met het bedrijfsleven ervan uitgaand dat eigenaren en exploitanten van CNI het best in staat zijn om hun risico's te beheersen. Ter bevordering van de samenwerking en het uitwisselen van informatie wordt het *Trusted Information Sharing Network* (TISN) gebruikt. Binnen dit webforum werken eigenaren en exploitanten samen en delen informatie. Het TISN besteed aandacht aan alle mogelijke risico's waaronder terrorisme, natuurgeweld, pandemie, cyberaanvallen en criminele activiteiten. Daarnaast onderneemt de Australische overheid diverse activiteiten om het bewustzijn te verhogen ten aanzien van onderlinge (*cross-sectoral*) afhankelijkheden, zoals in gezamenlijke oefeningen en werksessies met de industrie en in een *Critical Infrastructure Program for Modelling and Analysis*.

Het **Verenigd Koninkrijk** verdeelt de aanpak ter bescherming van CNI tegen terrorisme, natuurrampen en cyber security over verschillende programma's welke met name zijn beschreven in de *UK's counter-terrorism strategy* (CONTEST), de *UK Cyber Security Strategy* en het *National Cyber Security Programme*. Een strategisch kader is opgesteld in de CNI Protection in the UK: *Framework and Guidance*. Ten aanzien van CNI richt het CONTEST-programma zich op het vergroten van de veerkracht, nauwe samenwerking met de private sectoren, creëren van generieke capaciteiten, voorbereiding en oefenen. Binnen de diverse programma's is vooral aandacht voor de continuering en verbetering van security en bedrijfscontinuïteit in

de energie- en watersectoren en calamiteiten veroorzaakt door overstromingen of "ruimteweer".

Denemarken heeft de aanpak van de bescherming van CNI tegen terrorisme, spionage, natuurrampen en cyber security verdeeld over verschillende organisaties. Daarbij onderschrijft Denemarken een sterke sectorale benadering om maatwerkoplossingen te creëren in plaats van algemene wetgeving voor te schrijven. Denemarken werkt samen met omringende landen Finland, IJsland, Noorwegen en Zweden in de *Nordic cooperation*.

Alle onderzochte landen hebben een nationale strategie ter bescherming van vitale infrastructuur opgesteld. Wellicht niet met zo veel woorden maar alle strategieën benadrukken de aspecten:

- leiderschap;
- samenwerking;
- resultaatgerichtheid.

Opvallend is dat de meeste strategieën spreken over *critical infrastructure resilience* (CIR) in plaats van het eerder gebruikelijke *critical infrastructure protection* (CIP). Dit kenmerkt een verschuiving in aanpak van het creëren van voldoende weerstand (bescherming en voorkomen van incidenten) naar een aanpak die meer nadruk legt op de veerkracht van de CNI en het omgaan met verstoringen door de eigenaren en exploitanten van CNI. Overigens verstaan de verschillende definities onder veerkracht nog steeds de begrippen weerstand, betrouwbaarheid, redundantie en reactie en herstel.

De focus van alle landen ligt op de bescherming van CNI tegen terrorisme en cyberaanvallen. Echter in de uitvoering kennen de landen grote sectorale verschillen in volwassenheid, aanpak en wetgeving. De bestrijding van natuurrampen en calamiteiten is meestal apart benoemd en belegd bij andere organisaties. Wetgeving is summier. Harde beveiligingseisen ontbreken in wetgeving. Wetgeving beperkt zich op dit terrein over het algemeen tot kaderstellende richtlijnen.

Alle nationale strategieën en actieplannen hebben als gemeenschappelijke deler:

- focus op het bevorderen van de veerkracht;
- hanteren van een alles omvattende (holistische) risico-gebaseerde aanpak;
- een integrale aanpak van cybersecurity bij de bescherming van CNI;
- focus op de bescherming van industriële controle systemen (ICS, SCADA) binnen CNI;
- vergroten van het begrip ten aanzien van onderlinge afhankelijkheden en cascade-effecten;
- vergroten van de betrokkenheid en bewustwording ten aanzien van CNI-problemen;
- bevorderen van het gebruik van bestaande normen en praktijkrichtlijnen;
- opbouwen van (herstel)capaciteit en paraatheid voor het omgaan met incidenten;
- jaarlijks beoefenen van (sector overstijgende) scenario's met bedrijfsleven en overheid.

De nationale strategieën benadrukken het belang en de verantwoordelijkheden van de private sectoren, eigenaren en exploitanten. Een rode draad in alle strategieën is de noodzaak voor een zinvolle inhoudelijke samenwerking én informatie-uitwisseling tussen betrokken partijen. In het bijzonder geldt dit voor publiek-private samenwerkingen. Gedeelde informatie moet tijdig, zinvol en opvolgbaar (*actionable information*) zijn.

VITALE INFRA EN EU-VOORZITTERSCHAP 2016

Mathilda Buijtendijk en Sladjana Cemerikic
Ministerie van Veiligheid en Justitie, NCTV

Vitale infrastructuur stopt niet bij de grens. Door de vergaande Europeanisering en globalisering van de samenleving zijn de vitale producten, diensten en processen steeds meer vervlochten met internationale systemen. Vitale infrastructuur is dan ook internationaal een belangrijk thema. Nederland is al jaren op dit terrein actief, zoals in Europa via het Europese programma voor de bescherming van vitale infrastructuur (EPCIP).

Binnen de Europese Unie valt dit thema onder de raadswerkgroep Civiele bescherming. Als EU-voorzitter in de eerste helft van 2016 zal Nederland binnen deze raadswerkgroep de aandacht voor bescherming van vitale infrastructuur vragen. Het thema van het Nederlandse voorzitterschap van deze werkgroep zal *resilient infrastructure* zijn. Nederland zal zijn voorzittersrol benutten om, conform nationaal beleid, de nadruk te blijven leggen op het belang van publiek-private samenwerking. Hiermee wil Nederland aan het volgende bijdragen.

Het vergroten van het bewustzijn dat de uitval van vitale infrastructuur een belangrijk thema is voor de civiele bescherming in de lidstaten, vanwege de grote impact op de samenleving.
Het verder versterken van deze relatie tussen civiele bescherming en vitale infrastructuur door bijvoorbeeld in een oefening te demonstreren wat de cascade-effecten zijn van de uitval van vitale infrastructuur en welke gevolgen dat heeft voor de autoriteiten belast met civiele bescherming.
Het op gang brengen van een dialoog over de risico's die vitale infrastructuur bedreigen (zoals overstromingen). Hierbij kan zowel het aspect van het maken van risicoanalyses aan de orde komen als het delen van de belangrijkste lidstaat-overstijgende risico's voor de vitale infrastructuur.
Ten slotte het delen van informatie over hoe de weerbaarheid van deze vitale infrastructuur vergroot kan worden en deze deel te laten uitmaken van het risicomanagement van lidstaten.

Nationale veiligheid in een woelige wereld

De nationale veiligheid wordt steeds meer door ontwikkelingen in de internationale omgeving bepaald. Een blik op de Nationale Risicobeoordeling laat zien dat niet zozeer rampen, maar vooral crises een relatie met het buitenland hebben. Voor die internationale omgeving komt steeds meer belangstelling. In deze bijdrage bespreek ik enkele nieuwe publicaties die de discussie over Nederland in een woelige wereld moeten aanjagen.

Rob de Wijk
Hoogleraar Internationale Betrekkingen, Campus Den Haag Universiteit Leiden en directeur Den Haag Centrum voor Strategische Studies

Natuurlijk kunnen rampen en crises van binnenlandse oorsprong zijn, zoals de Vuurwerkramp die op 13 mei 2000 in Enschede plaatsvond. Of de (bijna) crisis die ontstond toen in 2002 de politicus Pim Fortuyn werd vermoord. De Nationale Risicobeoordeling (NRB) toont echter aan dat het merendeel van de risico's "geïmporteerd onheil" is. Overstromingen en extreme weerscondities kunnen het gevolg zijn van de mondiale verandering van het klimaat. Extremisme en polarisatie kunnen verbonden zijn met de gebeurtenissen in Syrië en Libië. En verstoringen van het ICT-netwerk kunnen het gevolg zijn van hacks uit China, Rusland of andere landen.

VOORTGANGSBRIEF NATIONALE VEILIGHEID

De NRB, als onderdeel van de Strategie Nationale Veiligheid (SNV), is een geweldig hulpmiddel om het debat over wat ons bedreigt, gestructureerd te voeren. Hier ligt een belangrijke taak voor het ministerie van Veiligheid en Justitie nu die NRB wordt vervangen door een Nationaal Risicoprofiel dat eens per vier jaar wordt vastgesteld. Minister Van der Steur schrijft in de *Voortgangsbrief Nationale Veiligheid* van 12 mei jl. dat zich in die vier jaar natuurlijk nieuwe risico's aandienen die geanalyseerd moeten worden en als "tussenproducten" moeten worden gecommuniceerd. Zo bezien wordt er gelukkig niet veel veranderd aan een uiterst nuttig instrument.

NRB en SNV zijn echter weinig bekend bij de professionals in het veld. Een mogelijke verklaring voor de onbekendheid is dat de gevolgen van de SNV voor die professionals beperkt zijn. De reden is dat de NRB nooit goed gebruikt is om de capaciteiten te bepalen voor rampenbestrijding en crisisbeheersing waarover Nederland moet beschikken.

Daarin lijkt nu verandering te komen. Hoopvol is dat de minister in zijn brief aankondigt dat het nieuwe risicoprofiel nu daadwerkelijk gebruikt gaat worden voor het bepalen van de capaciteiten die voor rampenbestrijding en crisisbeheersing nodig zijn. Dit was al de bedoeling van de in 2007 vastgestelde SNV, maar is nooit goed van de grond gekomen. Hopelijk wordt deze omissie nu rechtgezet, want verbeterd inzicht in de aard van de dreiging is betekenisloos als dit niet leidt tot verbetering van de capaciteiten om die dreigingen teniet te doen.

STRATEGISCHE MONITOR

Nationale dreigingen kunnen alleen goed worden geduid als ze in een bredere internationale context worden beoordeeld. Alleen dan is het mogelijk om plausibele uitspraken over toekomstige ontwikkelingen in het risicobeeld te doen en met investeringen te

© Ministerie van Defensie

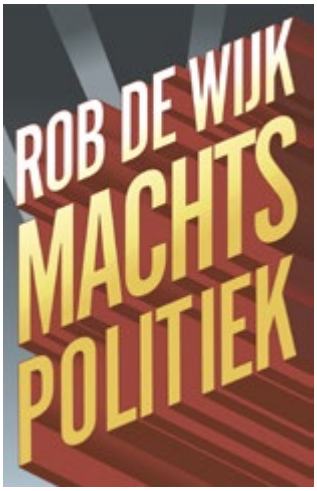
anticiperen op de dingen die komen gaan. Omgekeerd heeft ook het uitblijven van investeringen invloed op het risicobeeld. Door de financiële crisis dreigden kortingen op vitale infrastructuur waardoor Nederland onveiliger zou worden. Door de crisis nam ook het gevoel van onbehagen toe waardoor maatschappelijke dreigingen zoals polarisatie toenamen.

Het ministerie van Defensie heeft van alle ministeries de meeste ervaring met het maken van analyses om de toekomstige capaciteiten van de krijgsmacht te bepalen. Dit is sinds jaar en dag de kern van het defensieplanningssysteem. Voor de nationale veiligheid moet een dergelijk systeem met urgentie worden ontwikkeld.

Een goede ontwikkeling is dat ook het ministerie van Veiligheid en Justitie zich heeft aangesloten bij de ontwikkeling van de *Strategische Monitor* van de ministeries van Buitenlandse Zaken en Defensie.[1] De laatste versie van deze studies (die door Clingendael en het Den Haag Centrum voor Strategische Studies (HCSS) worden uitgevoerd en medio juni zijn verschenen) geeft inzicht in de laatste trends, feiten en cijfers. Interessant is te zien dat na een aanvankelijke daling van het aantal conflicten en het aantal slachtoffers dat viel, er sinds 2010 weer een stijging te zien is.

Het merendeel van de slachtoffers valt in 14 landen waar conflicten woeden; het merendeel in de buurt van Europa: Syrië, Irak, Libië, Oekraïne, Jemen, Somalië, Israël/Palestina en iets verder weg in landen als Nigeria en Zuid Soedan. De gevolgen van de nabijheid van deze conflicten laten zich raden: vluchtelingenstromen richting Europa; de opkomst van extremistische groepen; steeds nauwere verwevenheid tussen de internationale criminaliteit; extremistische groepen en de vluchtelingenproblematiek (mensensmokkelaars). Als gevolg hiervan is er politieke onenigheid binnen Europa over de aanpak van deze problemen en maatschappelijke polarisatie en onbehagen als gevolg van de perceptie van landen die door vluchtelingen overspoeld worden en de wereld onveiliger. Dat dit zich vertaalt in aard en omvang van in de NRB en het toekomstige Nationaal Risicoprofiel beschreven risico's behoeft geen betoog.

Tegelijkertijd nuanceert de Strategische Monitor. De onveiligheid rond Europa mag dan hoog zijn; de veiligheid in grote delen van de wereld neemt juist toe. Bovendien neemt de samenwerking tussen landen zeker niet af en is er in de wereld veel meer sprake van samenwerking dan van conflict. En 80% van de slachtoffers van terrorisme vallen in vijf landen: Syrië, Nigeria, Pakistan, Irak en Afghanistan, terwijl het aantal aanslagen in Europa de afgelopen jaren uiterst beperkt was, ook al was de schok over de aanslag op Charlie Hebdo in Parijs in januari 2015 groot.



MACHTSPOLITIEK

Nieuw is de discussie over de trends op mondiaal niveau: het ontstaan van een gefragmenteerde wereld met meerdere, elkaar beconcurrerende machtscentra. Over de machtspolitiek die daarvan het gevolg is, gaat mijn eigen *Machtspolitiek* dat begin juni verscheen.[2] De conclusie van dit boek is dat de wereld zoals wij die kennen in hoog tempo verandert, dat die wereld veel meer volgens de voorkeuren van opkomende landen als China zal worden gemodelleerd en dat de conflicten die momenteel escaleren in de Zuid Chinese Zee en het huidige conflict met Rusland over Oekraïne, passen in een beeld van toenemende mondiale onveiligheid. Kortom, de wereld wordt instabieler. Dat dit nieuwe veiligheidsrisico's voor Nederland oplevert, is helder.

De *Strategische Monitor* en inzichten zoals ik die in *Machtspolitiek* presenteer beschrijven de context voor het Nationale Risicoprofiel. Ze geven inzicht in toekomstige risico's en de verschuivingen in de impact en waarschijnlijkheid van bestaande risico's.

Dit soort inzichten moet leiden tot een nieuwe visie op de risico's voor Nederland, nieuwe prioriteiten in de crisisbeheersing, de rol van de krijgsmacht en de prioriteiten in het buitenlandbeleid. Van even groot belang is een Kabinetsbrede visie op economische groei in een wereld die gedomineerd wordt door opkomende machten. Economische groei is essentieel om onze welvaart en daarom onze veiligheid op peil te houden.

Dit alles vereist een geavanceerd systeem van risicoanalyse, gekoppeld aan een werkbare methode om de toekomstige capaciteiten te bepalen voor rampenbestrijding en crisisbeheersing, maar ook voor de krijgsmacht. Juist door grote veranderingen die mondiaal plaatsvinden, wordt dit belangrijker dan ooit. Dit vergt allereerst volop investeren in kennis. Dit is een notitie die alom gedeeld wordt, maar nog te weinig in de praktijk wordt gebracht.

[1] De Strategische Monitors van Clingendael en HCSS zijn op 10 juni aan de minister van Defensie gepresenteerd. De gegevens komen uit het HCSS jaarrapport *The Return of Ghosts hoped past*?

[2] Rob de Wijk, *Machtspolitiek*, Amsterdam: Amsterdam University Press, 2015.

DE TERUGKEER VAN OUDE SPOKEN?

Mondiale trends in conflict en samenwerking

Kelsey Shantz, Frank Bekkers, Stephan de Spiegeleire en Tim Sweijs
Den Haag Centrum voor Strategische Studies (HCSS)

Decennialang leefde Europa in vrede en voorspoed. Maar de afgelopen jaren doken de geesten uit een verleden dat we dachten achter ons gelaten te hebben weer op. Niet op afgelegen plekken als Afghanistan of in de Zuid-Chinese zee, maar steeds dichter bij de grenzen van Europa. Rusland annexeerde de Krim. Het ebolavirus zaaide dood en verderf in West-Afrika, maar wist ook Spanje en het Verenigd Koninkrijk te bereiken. En Europa moest geschokt toezien hoe verschillende Europese burgers zich aansloten bij IS en met de strijders mee vochten, slachtingen aanrichtten en om het leven kwamen. In de veiligheidsdebatten die momenteel gaande zijn, komt telkens weer naar voren dat sommige bijzonder kwade geesten uit het verleden zich weer op Europese bodem manifesteren. Het zijn zeker geen hersenschimmen en ze vormen een formidabele uitdaging.

Nederland staat dit jaar voor belangrijke keuzes voor het defensie- en veiligheidsbeleid van de komende jaren. Op welke veiligheidsrisico's moeten we ons voorbereiden in het licht van de recente ontwikkelingen? Welke capaciteiten zijn nodig om deze risico's te voorkomen en de kop in te drukken? Wanneer, waar en met wie moeten deze capaciteiten worden ingezet? En moet het veiligheids- en defensiebudget - dat al twee decennia een neerwaartse trend kent - hiervoor worden verhoogd?

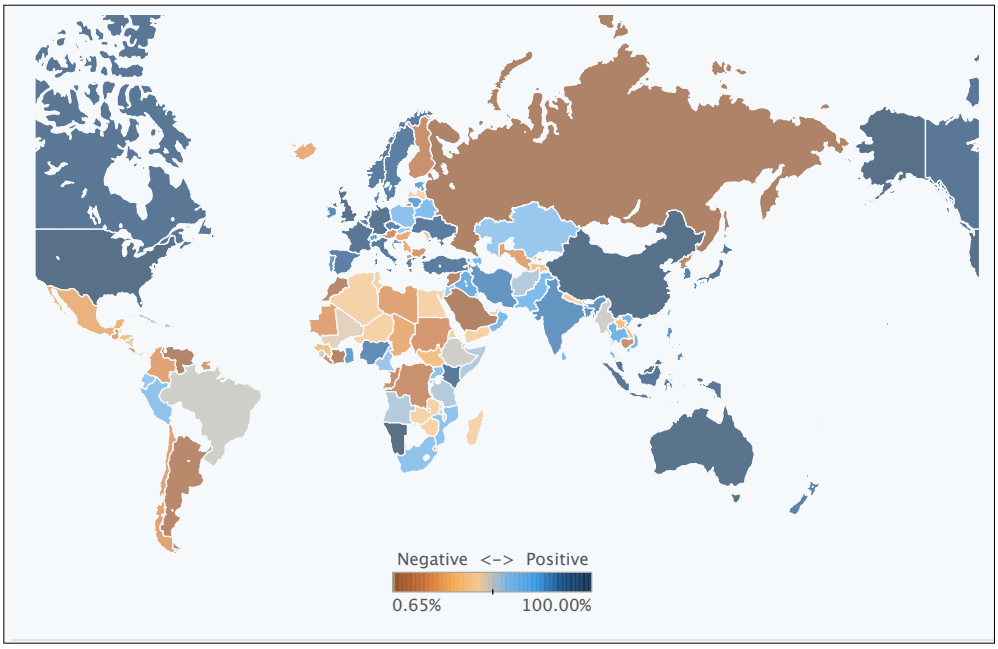
DE STRATEGISCHE MONITOR

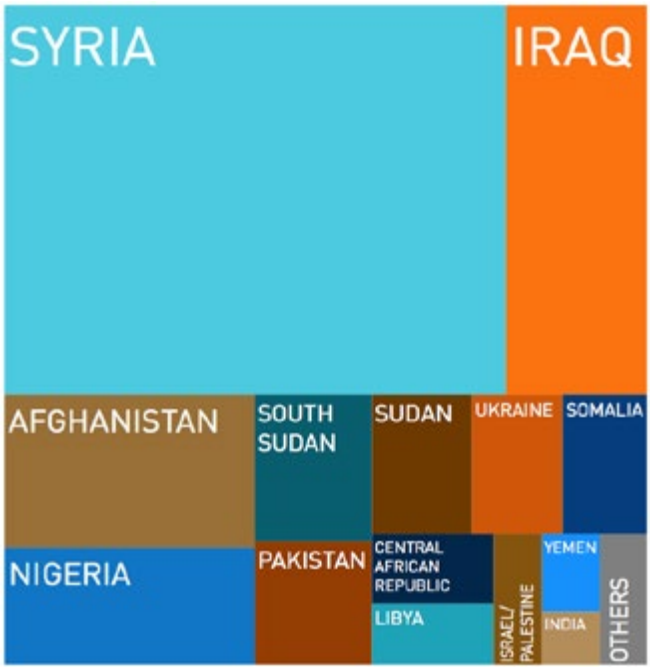
De grondslag voor het besluitvormingsproces voor deze en soortgelijke vragen wordt gevormd door het zorgvuldig onderzoeken en analyseren van de mondiale veiligheidssituatie van vandaag. De Nederlandse ministeries van Defensie, Buitenlandse Zaken en Veiligheid en Justitie hebben daartoe de Strategische Monitor ingesteld, in samenwerking met het Nederlands Instituut voor Internationale Betrekkingen Clingendael en Den Haag Centrum voor Strategische Studies (HCSS). De Strategische Monitor is, in de woorden van minister Hennis van Defensie, een "cruciaal handvat" voor de ontwikkeling van het Nederlandse veiligheids- en defensiebeleid.

Het woord *monitor* komt van het Latijnse werkwoord *monere*, dat wil zeggen "manen, waarschuwen, adviseren". Dit houdt in dat een Monitor niet alleen observaties moet bevatten, maar ook waarschuwingen of zelfs tegendraadse opvattingen om besluitvormers te wijzen op trends en ontwikkelingen die ze nog wel eens missen, negeren of naast zich neerleggen. En dat is precies waar HCSS sinds zijn eerste bijdrage aan de Strategische Monitor in 2012 naar streeft. We pleiten ervoor de steeds complexer en dynamischer *future space* vanuit verschillende perspectieven te benaderen en werken daar ook aan. Zo heeft HCSS een goed gevulde portfolio ontwikkeld (en blijft deze verder ontwikkelen) van datasets, tools en methoden om analytische inzichten te verstrekken ter ondersteuning van de strategische besluitvorming op het gebied van defensie en veiligheid.

In het rapport *The Return of Ghosts Hoped Past? Global Trends in Conflict and Cooperation*, HCSS' recentste bijdrage aan de Strategische Monitor, wordt de lange termijn impact van weer opduikende spoken uit het verleden op de veiligheid onderzocht. Maar zijn de gruwelijke gebeurtenissen die in 2014 het nieuws beheersten, zoals het neerhalen van MH17 en de gewelddadigheden van Islamitische Staat, geïsoleerde incidenten of onderdeel van een structurele trend? In het rapport heeft HCSS recente gebeurtenissen en trends onder de loep genomen in het licht van overkoepelende conflictpatronen.

Assertiviteit andere landen richting Nederland in 2014





Dodelijke slachtoffers in de top 20 van de dodelijkste conflicten in 2014[1]

TRENDS IN CONFLICTEN

Tussen 1990 en het begin van deze eeuw is het aantal interstatelijke en intra statelijke conflicten drastisch verminderd, maar aan deze neerwaartse trend bij gewapende conflicten is sindsdien een einde gekomen. Het aantal mensen dat jaarlijks in de gewapende strijd om het leven komt is het afgelopen decennium gestegen als gevolg van de voortdurende onrust in de periferie van Europa. In Syrië, Irak en Afghanistan werden van 2013 tot 2014 de dodelijkste oorlogen gevoerd waarbij in alle drie de landen het aantal dodelijke slachtoffers toenam; ook de burgeroorlog in Oekraïne bracht grote verwoestingen teweeg. In het afgelopen decennium is ook het aantal terroristische bomaanslagen met veel slachtoffers (15 doden of meer) gestegen; 80% van de slachtoffers kwam in slechts vijf landen om het leven: Syrië, Nigeria, Pakistan, Irak en Afghanistan. Een voor Europa bijzonder verontrustende ontwikkeling is de besmetting en *spill-over* van conflicten die momenteel woeden in de Sahel, het Midden-Oosten, Noord-Afrika en Zuidwest-Azië. Een andere ontwikkeling is het samenvloeien van verschillende soorten conflicten. De deelname van transnationale gewapende bewegingen aan interne gewapende conflicten verandert de lokale dynamiek van een conflict en de reikwijdte en de aard ervan, zoals de aanslag op Charlie Hebdo aantoont. Het is bepaald niet gemakkelijk de tegenstander te identificeren en een strategisch zwaartepunt te definiëren.

RUSLAND: VAN ASSERTIEF TOT AGRESSIEF

De toenemende assertiviteit die Rusland het afgelopen decennium aan Europa's oostgrenzen aan de dag legde, is nu uitgegroeid tot regelrechte agressie. In 2014 bleek Rusland het eerste Europese land dat sinds het einde van de Tweede Wereldoorlog door middel van dreiging en de inzet van het leger zijn eigen grondgebied uitbreidde ten koste van een ander Europees land. Deze strategische zet van Rusland dwingt veiligheids- en defensieorganisaties de situatie met nieuwe ogen te bekijken. Rusland vertegenwoordigt een uiterst ingewikkelde uitdaging omdat de dreiging wordt gevormd door een samenspel van hoogwaardige militaire capaciteiten en andere niet-militaire dreigingen. De onmiddellijke uitdaging die Rusland vormt zou moeten leiden tot een fundamentele heroverweging van de wijze waarop veiligheids- en defensieorganisaties hun strategische planning vormgeven.

HET IS NIET ALLEMAAL KOMMER EN KWEL

Hoewel het geweld aan Europa's grenzen en de Russische agressie de zorgen doen toenemen, ziet niet alles er even somber uit. Nederland ziet tekenen van een positieve interactie en een op samenwerking gerichte dialoog vanuit Europese naties, zoals blijkt uit een geautomatiseerde analyse van "samenwerkingstaal" tussen naties. Bij deze analyse werd gebruik gemaakt van de Global Database of Events, Language and Tone (GDELT). Ondanks de verdeeldheid binnen de Unie blijft Europa in vergelijking met de rest van de wereld een baken van stabiliteit binnen de internationale samenwerking. Nederland speelt een centrale rol op het gebied van steun en samenwerking binnen de internationale gemeenschap en de twee toonaangevende landen in het internationale stelsel, de Verenigde Staten en China, staan in de top twee percentiel van landen met de meest positieve houding ten opzichte van Nederland.

KORTOM

De verschillende uitdagingen op veiligheidsgebied waarmee Europa wordt geconfronteerd zijn harde realiteit. Het betreft niet zozeer geïsoleerde incidenten, als wel een bredere trend. De uitdagingen vergen onmiddellijke aandacht maar ook creatieve oplossingen. Maar zoals Albert Einstein al opmerkte, we kunnen onze problemen niet oplossen met de denkwijze die deze heeft veroorzaakt. We moeten opnieuw investeren in onze defensie- en veiligheidscapaciteiten om het hoofd te bieden aan de veiligheidsuitdagingen die aan onze oost- en zuidgrenzen opdoemen. Maar tegelijkertijd moeten we ook nadenken over een bredere portfolio van instrumenten waarmee we invloed kunnen uitoefenen, waaronder mechanismen om het internationale stelsel en de positieve trends die er tussen de onrustbarende ontwikkelingen door uit te destilleren vallen, te versterken.

[1] "Death Toll in 2014's Bloodiest Wars Sharply Up on Previous Year." Project for the Study of the 21st Century, 17 maart, 2015. http://projects21.com/2015/03/17/death-toll-in-2014s-bloodiest-wars-sharply-up-on-previous-year/

Is **Rusland** ontketend?

Stephan de Spiegeleire
Den Haag Centrum voor Strategische Studies

2014 vormde een keerpunt in de relatie tussen de Russische Federatie en het Westen. In zijn bijdragen aan de Strategische Monitor van de Nederlandse overheid maakt HCSS al enkele jaren gewag van de toenemende internationale assertiviteit van Rusland. Dit jaar moeten we concluderen dat deze assertiviteit in een andere categorie is beland: die van onverholen agressie. Rusland is het eerste Europese land dat na het einde van de Tweede Wereldoorlog zijn eigen grondgebied met geweld heeft uitgebreid. 2014 was ook het jaar waarin de Russische agressie in Nederland hard aankwam. Bijna 200 Nederlanders werden het slachtoffer (MH17) van een conflict waarbij, zoals ook president Poetin heeft toegegeven, Rusland direct betrokken was. Voor een land dat jarenlang goede banden met Rusland heeft gekoesterd en dat zich tot het uiterste heeft ingespannen om de Russische transitie te steunen kwam dit als een grote schok die nog lang gevoeld zal worden.

Rusland is in een bijzonder gevaarlijke fase beland in zijn "transitie" waarbij men het bestuur, de economie, de maatschappij en het leger van de Sovjetstijl wil ontdoen. Deze andere houding van Rusland werd het Westen onmiddellijk duidelijk toen het land in het conflict in Oekraïne een agressiever buitenland- en veiligheidsbeleid ging hanteren. In ons rapport besteden we echter ook aandacht aan de onheilspellende veranderingen in het *militaire* domein in Rusland zelf. Alle Russische diensten, waaronder de nog steeds cruciale strategische kernmacht, hebben in 2014 ongekende hoeveelheden nieuw materieel gekregen. De algehele staat van paraatheid is aanzienlijk verbeterd dankzij grootschalige militaire oefeningen in 2014. Deze aantallen, geografische reikwijdte en intensiteit hebben we sinds de val van de Sovjet-Unie niet meer gezien en de kloof met de geoefendheid/paraatheid van de NAVO-landen (waaronder Nederland) groeit. Het schokkendst is nog de wijze waarop de Russische leiders trachten - en erin lijken te slagen - de Russische samenleving te militariseren waarin helaas weinig weerstand bestaat tegen de behoorlijk geraffineerde patriottische propagandamachine.

Al dit borstgeroffel vindt plaats op een moment waarop de diepgewortelde systeemzwakte van de Russische economie en staat steeds duidelijker aan het licht komt. De economie leunt onevenredig zwaar op de olie- en gasexport in een tijd waarin mondiale technologische doorbraken voor een radicaal andere energiesector en evenwichtiger speelveld zullen zorgen. Een elite die ongebreideld kan profiteren, systemische corruptie in de maatschappij en de volstrekt ineffectieve top-down bestuursstructuur hebben de Russische samenleving en staat tot in hun vezels verzwakt. De negatieve gevolgen van dit alles waren al vóór 2014 zichtbaar. De daling van de olieprijs en de gevolgen van Westerse sancties hebben de kans op nieuwe schokken vergroot. Rusland beschikt nog wel over financiële buffers die in de jaren van overvloed zijn aangelegd, maar we moeten ons erop voorbereiden dat de grote buur van Europa op korte en middellange termijn nóg roeriger tijden gaat doormaken.

2014 was een duidelijke wake-up call. Onze veiligheids- en defensieorganisaties moeten Rusland en de nieuwe uitdagingen waarvoor dit land ons stelt veel serieuzer gaan nemen. We zullen ons moeten verdiepen in hoe we om moeten gaan met deze nieuwe combinatie van "oude" (nucleaire, conventionele kinetische, directe) en nieuwe (hybride, niet-kinetische, indirecte) militaire uitdagingen in termen van preventie en reactie en in termen van afschrikking en dwang. Na het uiteenvallen van de Sovjet-Unie konden militairen en veiligheidsdiensten de near-peer concurrentie (in militaire termen) in hun toekomstscenario's nog bagatelliseren. Deze luxe kunnen we ons niet meer veroorloven. Maar we moeten ons wel realiseren dat de veiligheidsrisico's (en mogelijkheden!) waarvoor Rusland ons stelt fundamenteel anders zijn dan die in het Sovjettijdperk. Nu moeten we in deze nieuwe situatie echter niet schielijk terugkeren naar de defensieve capaciteiten, beleidsprioriteiten en mindset van de Koude Oorlog. Wat we nu nodig hebben is een creatiever, breder (gehele overheid/maatschappij) en - eerlijk gezegd - strategischer debat over een nieuwe en evenwichtiger portfolio van mogelijkheden, opties en (ecosysteem)partners.

Barbarij en religie

Kelsey Shantz en Tim Sweijs
Den Haag Centrum voor Strategische Studies

De huidige conflictgebieden vormen regelrechte internationale "finishing schools" voor extremisten[1], aldus een zeer recent rapport van de VN Veiligheidsraad. Naar schatting hebben 25.000 terroristische strijders uit ruim 100 landen zich begeven op de strijdtonelen in het Midden-Oosten.
Maar het religieuze geweld beperkt zich niet tot deze regio. Het vormt een wereldwijd probleem met ernstige gevolgen voor de Europese en Nederlandse binnenlandse veiligheid. In het onderzoek *Barbarism and Religion: The Resurgence of Holy Violence* wordt een nieuwe dataset gepresenteerd over religieus geweld gedurende de afgelopen 25 jaar. Gekeken is naar mondiale trends en ontwikkelingen en onderzocht hoe religieus geweld begint en weer eindigt. Verder zijn de belangrijkste uitdagingen geïdentificeerd voor organisaties belast met defensie en veiligheid.

Het religieuze geweld is de afgelopen 25 jaar toegenomen en steeds meer dodelijke slachtoffers gaan eisen. Niet alleen is de intensiteit toegenomen, ook de omvang en geografische reikwijdte zijn enorm gegroeid van Tsjaad tot China en van Myanmar tot Mali. Door religieus geweld zijn conflicten die voorheen gescheiden waren, gaan samenvloeien en lokale en mondiale gevoelens van wrok opgelaaid. Nationale grenzen worden steeds vaker overschreden, nu de gewelddadige jihad een steeds globalistischer karakter heeft gekregen. Verder neemt de strijd tussen militante extremistische groeperingen wereldwijd alarmerende vormen aan.
Religieuze extremisten die overgaan tot geweld in de naam van Allah, Boeddha, God of een ander opperwezen hanteren zeer strikte normen en waarden en zijn bereid tot grote persoonlijke offers om hun doelstellingen te verwezenlijken. In dit opzicht wijken ze af van de gebruikelijke actoren in conflicten. Religieuze conflicten houden daarom vaak langer aan dan gewone omdat men minder bereid is tot compromissen. Religieuze conflicten gaan bovendien vaker gepaard met ernstiger vormen van geweld, vooral tegen burgers.

De wortels van religieus geweld vertonen echter ook grote overeenkomsten met die van niet-religieus geweld, zoals zwakke staten, rechteloosheid, facties, repressie en sociale uitsluiting. Hoewel er weinig causale verbanden kunnen worden gelegd, vallen er wel gemeenschappelijke patronen te herkennen die leiden tot verschillende vormen van geweld, zoals de maatschappelijke kenmerken van religieuze verschillen in combinatie met opsplitsingen binnen groepen, bijvoorbeeld vanwege horizontale sociaaleconomische ongelijkheid, uitsluiting en repressie en de geografische afstand tussen religieuze groeperingen. De verschillen tussen religies worden gepolitiseerd, hetgeen kan leiden tot toenemende polarisatie tussen groepen en de kans op geweld vergroot.
Spanningen tussen religieuze groepen kunnen weliswaar uitmonden in conflicten, maar meerdere religies binnen een maatschappij vormen niet automatisch aanleiding voor religieus geweld. Het zijn vooral horizontale sociaaleconomische ongelijkheid en religieuze afsplitsingen die de kans op het uitbreken van conflicten vergroten met ongeveer een factor drie. Wanneer er dan bovendien extremistische actoren opduiken, kunnen die de lont in het kruitvat vormen. Er vallen individuele en situationele factoren te herkennen die individuen bevattelijker maken voor extremistische overtuigingen, maar er bestaat zeker geen *one-size-fits all*-profiel.

Religieus geweld neemt af zodra militante groeperingen met militaire middelen worden verslagen, hun operationele mogelijkheden drastisch worden ingeperkt en de strijdende groepen fysiek van elkaar gescheiden worden. Andere gunstige ontwikkelingen zijn vergrijzing, deradicalisering van belangrijke leden en groepen na onderhandelingen en akkoorden toelaten tot de reguliere politieke processen. Religieus geweld is niet alleen een probleem van deze tijd, maar zal dat voorlopig ook blijven. De komende jaren zullen de grote aantallen buitenlandse strijders en hun grote toewijding aan de zaak de veiligheid van burgers en regeringen overal ter wereld blijven bedreigen.

De aanpak van religieus geweld vergt een integrale maatschappelijke benadering met onder meer een centrale hoeder van de veiligheid die de pogingen tot stabilisering leidt en coördineert. Defensie- en veiligheidsorganisaties dienen eerst en bovenal meer inzicht te krijgen in het verschijnsel en de lokale cultuur.
Preventieve maatregelen zouden gericht moeten zijn op bevordering van de weerbaarheid van religieuze gemeenschappen tegen deze destructieve extremistische invloeden. De problemen dienen bij de wortel te worden aangepakt, met andere woorden dezelfde factoren die actoren ertoe bewegen zich aan te sluiten bij extremistische groeperingen. Uitsluitend wanneer religieuze groepen beschikken over substantiële conventionele militaire capaciteit is het gebruik van geweld gelegitimeerd om hun aanvoerlijnen te vernietigen en vluchtroutes te blokkeren. De effectieve aanpak van religieus geweld vergt doorgaans echter eerder overreding dan dwang en samenwerking in plaats van controle ten behoeve van de stabiliteit op de lange termijn - zowel in de conflictregio's als in eigen land.

[1] "De VN en de Veiligheidsraad herhalen hun voornemen buitenlandse terroristische strijders aan te pakken." UN News Centre, 29 May 2015.

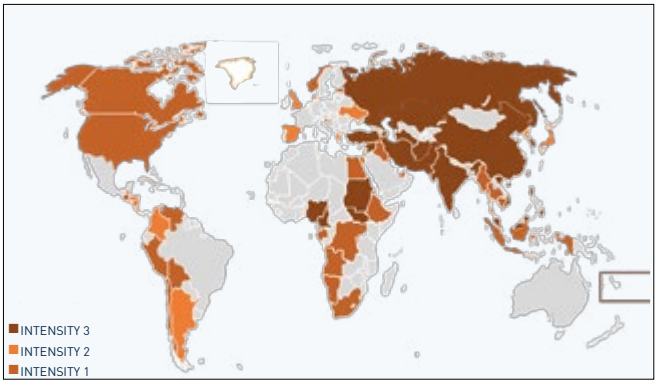
Waarom wordt er in de 21ste eeuw nog om land gevochten?

Willem Th. Oosterveld, Tim Sweijs en Stephan de Spiegeleire
Den Haag Centrum voor Strategische Studies

In een tijdperk dat wordt gedomineerd door cyberspace, netwerken en de notie van een *global village* lijkt het voeren van oorlog om land iets te zijn dat tot de geschiedenis behoort. Dit sentiment vond een echo in de uitspraak van John Kerry daags na de inname van de Krim door de Russische president Poetin: "Het kan niet zo zijn dat je je in de 21ste eeuw gedraagt alsof het nog de 19e eeuw is en een stuk land inpikt op basis van valse voorwendselen." Vanuit het Westen bezien lijken territoriale conflicten dus een anomalie te zijn. Het tegendeel is echter waar: territoriale conflicten zijn nog volop aanwezig en beperken zich allerminst tot Oost-Europa of zelfs het Midden-Oosten.

In het Westen zijn we vaak geneigd om conflicten te beschouwen vanuit een etnisch of religieus perspectief en zijn we bijna vergeten dat land vaak een cruciale rol speelt in disputen tussen staten. Op basis van recent onderzoek van HCSS is gebleken dat maar liefst 51 van de 89 bestaande interstatelijke disputen een territoriale component heeft. Bij meer dan de helft van deze 51 conflicten bestaat er ook een verband met andere factoren, zoals politiek-militaire overwegingen, economische gronden of etnisch-culturele achtergronden. Tot deze groep behoren geschillen zoals tussen Soedan en Zuid-Soedan, Thailand-Cambodja, China en landen rond de Zuid-Chinese Zee en het conflict tussen Oekraïne en Rusland. Maar niet alle territoriale disputen leiden altijd tot gewelddadigheden: 41 van de 51 territoriale disputen hebben in het afgelopen jaar niet tot geweldsuitbarstingen geleid, en vaak vallen hier ook "bevroren conflicten" onder. Voorbeelden zijn Peru-Chili, Spanje-VK (Gibraltar), Fiji-Tonga maar ook Japan-Rusland.

Maar als er nog zoveel bevroren conflicten zijn, waarom zouden we ons er dan druk om maken? Het antwoord hierop ligt besloten in het complex van factoren dat aanleiding kan zijn tot uitbarstingen van geweld. Onderzoek heeft bijvoorbeeld aangetoond dat het aan de macht zijn van een *hardliner* de kans op conflict aanzienlijk verhoogt en als er zich aan beide zijden van een dispuut *hardliners* bevinden, dan is de kans hierop zelfs 95%! Dit maakt dus dat waakzaamheid is geboden ten aanzien van politieke ontwikkelingen in landen die betrokken zijn bij een territoriaal dispuut. Maar ook andere factoren kunnen een escalerende werking hebben, zoals de ontdekking van nieuwe hulpbronnen of het opzwepen van etnische spanningen. Daarentegen heeft een wapenwedloop tussen twee landen maar een verwaarloosbaar effect op de kans dat er conflict uitbreekt in relatie tot ruzie over land.
De diversiteit van factoren maakt ook dat territoriale disputen overal in de wereld aanwezig zijn (zie figuur 1). Opmerkelijk genoeg is Europa – *pace* het conflict in Oekraïne – hierop de enige uitzondering: de enige territoriale geschillen waar Europese landen bij betrokken zijn betreffen de twist over de Noordpool, het langlopende Cyprusconflict, en de kwestie-Gibraltar. Voor een klein continent met relatief veel landen opeengepakt is dit een opmerkelijke bevinding en ondersteunt het de stelling dat Europa nog steeds profiteert van het naoorlogse vredesdividend. Verder zien we dat veel landen in Azië, waaronder de grootmachten China, Japan, India en Rusland allemaal bij territoriale disputen zijn betrokken en vaak bij meerdere tegelijk. Afrika huist verschillende disputen die in veel gevallen over natuurlijke hulpbronnen gaan maar tegelijkertijd lage geweldsniveaus met zich meebrengen. Dit geldt bijvoorbeeld voor Angola-DR Congo, Nigeria-Kameroen en Gabon-Equatoriaal Guinee.



Spreiding territoriale conflicten (2013) met intensiteit. 1=dispuut zonder geweld; 2= crisis zonder geweld, 3= dispuut met geweld)

WAT BETEKENT DEZE ANALYSE VOOR NEDERLAND?

Het *belangrijkste* is om meer bewustwording te kweken voor de gevaren die territoriale disputen met zich mee kunnen brengen.

Ten *tweede* kan het helpen om beleidsmatig meer te focussen op gebiedstwisten die voor Nederland belangrijk zijn. Behalve Oekraïne zijn dat ook de kwesties in de Zuid-Chinese Zee en de aaneengeschakelde conflicten in het Midden Oosten. Traditionele militaire instrumenten om geweld in te dammen of uitbraken te voorkomen spelen hierbij een belangrijke rol.

Ten slotte is er een rol weggelegd voor Nederland in het promoten van vreedzame geschillenbeslechting: het Internationaal Gerechtshof heeft al meerdere territoriale disputen weten bij te leggen, onder andere tussen Chili en Peru (2014) Burkina Faso en Niger (2013) en Nigeria en Kameroen (2002) en heeft nog een aantal andere op de rol staan. Strijd om territorium is dus niet iets uit het verleden. Ook in de 21ste eeuw zal het een niet te onderschatten factor blijven in internationale conflicten.

CLINGENDAEL MONITOR 2015

Een wereld zonder orde?

In welke richting ontwikkelt het mondiale bestel zich, in het bijzonder waar het de internationale machtsverhoudingen en stabiliteit betreft? Waar bevinden zich de belangrijkste "hot spots" van conflict en instabiliteit? In hoeverre is de internationale gemeenschap in staat om door middel van samenwerking orde binnen het internationale systeem te bewaren? En wat betekent dit alles voor Nederland en zijn partners en bondgenoten? Deze vragen staan centraal in de laatste versie van de Clingendael Monitor die dit voorjaar is verschenen onder de titel "Een wereld zonder orde"?[1]

Jan Rood, Frans-Paul van der Putten en Minke Meijnders
Instituut Clingendael, afdeling Onderzoek

De Clingendael Monitor vormt een voortzetting van het interdepartementale project "Verkenningen; houvast voor de krijgsmacht van de toekomst" dat in 2010 zijn eindrapport opleverde. Deze editie bouwt daarnaast voort op eerdere versies van de Clingendael Strategische Monitor.[2] Doel van de monitorexercitie is om huidige ontwikkelingen en verwachte toekomstige trends (met een termijn van 5 à 10 jaar) binnen het internationale bestel te analyseren en in kaart te brengen, in het bijzonder ontwikkelingen die relevant zijn voor de Nederlandse (en Europese) veiligheid. Daarbij beoogt de Clingendael Monitor – geschreven in opdracht van de ministeries van Defensie, Buitenlandse Zaken en Veiligheid en Justitie - beleidsmakers te ondersteunen bij het formuleren van toekomstig beleid in nationaal, Europees en bondgenootschappelijk en multilateraal verband.

Wat zijn volgens de laatste Clingendael Monitor de belangrijkste ontwikkelingen en wat betekenen deze voor de internationale verhoudingen?

MACHTSVERSCHUIVINGEN EN MOEIZAMER INTERNATIONALE SAMENWERKING

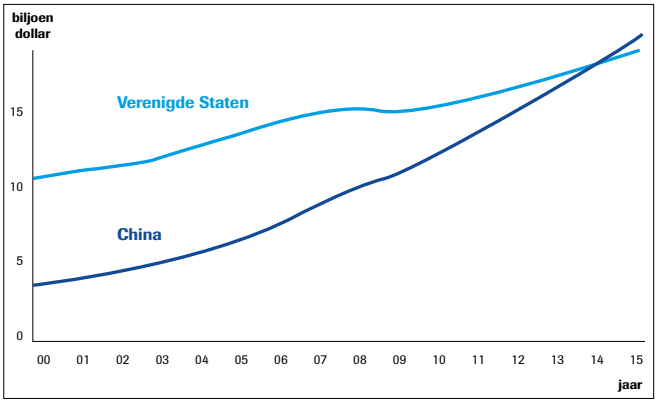
De in de eerdere edities van de Monitor geschetste herschikking van de mondiale machtsverhoudingen zet door, waarbij steeds duidelijker wordt dat China (met op de achtergrond India en Brazilië) de belangrijkste opkomende macht is. China is nu al de VS gepasseerd als grootste economie en passeert in 2015 de VS ook als grootste buitenlandse investeerder. Daartegenover staat dat de VS vooralsnog militair de machtigste mogendheid blijven. Maar dit beeld onderstreept een ontwikkeling naar een meer multipolaire wereld, met als implicatie een afnemende macht van het Westen (de VS en de EU) en daarmee een afnemend vermogen van westerse landen om het mondiale systeem te beheersen.

Mede als gevolg van de gaande machtsverschuiving verloopt Internationale samenwerking, al dan niet in multilaterale kaders, moeizamer. Samenwerking is daarbij steeds sterker afhankelijk van de opstelling van de grote mogendheden. Kunnen zij tot overeenstemming komen, dan blijkt gemeenschappelijk optreden mogelijk. Vaker wordt de samenwerking echter belemmerd door belangentegenstellingen, machtspolitieke rivaliteit en conflicten. Voor zover samenwerking plaatsvindt, is deze ad-hoc en minder institutioneel verankerd. Deze ontwikkeling is eigen aan een wereld die qua orde en verhoudingen in de overgangsfase verkeert van een Westers gedomineerd bestel naar een orde waarbinnen opkomende landen hun plaats opeisen en waarop zij hun stempel proberen te drukken. De tegenstellingen spitsen zich daarbij toe op de waarden en beginselen die aan het mondiale bestel ten grondslag liggen en op de zeggenschapsverhoudingen binnen de bestaande multilaterale kaders (VN, IMF, Wereldbank etc.). Het Westen, de VS in het bijzonder, staat hierbij tegenover opkomende en revisionistische landen, waarbij vooral China en Rusland elk op hun eigen manier verandering van de bestaande orde nastreven. In het geval China vertaalt dit zich onder andere in de oprichting van alternatieve c.q. rivaliserende (regionale) economische instituties.[3] Een gevolg hiervan is dat de klassieke Nederlandse inzet op een "rule-based international order" onder druk staat.

[1] Jan Rood, Frans-Paul van der Putten en Minke Meijnders, *Een wereld zonder orde?; Clingendael Monitor 2015*. Den Haag: Instituut Clingendael, februari 2015.

[2] Jaïr van der Lijn en Andrea Teftedarija (eindred.), *Continuïteit en onzekerheid in een veranderende wereld; Clingendael Strategische Monitor 2012*. Den Haag: Instituut Clingendael, 2012; Jan Rood en Rosa Dinnissen (eindred.), *Een wereld in onzekerheid; Clingendael Strategische Monitor 2013*. Den Haag: Instituut Clingendael, 2013; Jan Rood (eindred.), *Een wankele wereldorde; Clingendael Strategische Monitor 2014*. Den Haag: Instituut Clingendael, 2014.

[3] Zie in het bijzonder het Chinese initiatief voor een Aziatische Infrastructuur Investeringsbank en de in 2013 opgerichte BRICS-Bank.



Chinese 'takeover': totale inkomen in koopkrachtpariteit China vs. de VS
'The World in Transition', In: The Economist. November 2014, p. 90.

De Monitor 2015 laat zien dat als gevolg hiervan het internationale bestel op het breukvlak staat van enerzijds een meer geopolitieke wereld – waarbinnen rivaliteit, conflict en (economische) blokvorming overheersen – en anderzijds de wereld van de *interdependentie* – waarin op basis van onderlinge afhankelijkheid samenwerking mogelijk blijkt te zijn. In welke richting dit wereldbestel zich zal ontwikkelen, is daarbij sterk afhankelijk van de Chinees-Amerikaanse relatie: de belangrijkste as binnen het zich ontwikkelend wereldsysteem. De uitdaging voor Europa is om in dit assenspel een eigen plek te vinden.

INSTABILITEIT EN CONFLICTEN: HET MONDIALE DREIGINGSBEELD

De wereld van de geopolitiek komt, zo laat de Monitor 2015 zien, het sterkst naar voren in de vorm van toenemende (territoriale) spanningen tussen de grote mogendheden, direct dan wel via "proxys".

Eén van de "hot spots" is Oost-Azië, waar de regionale hegemoniale ambities en bewegingen van China botsen met de naoorlogse positie van de VS als "security provider" voor onder andere Japan, Zuid-Korea, de Filippijnen en Taiwan. Hier tekenen de contouren zich af van een "Koude Oorlog" systeem, inclusief een vooral maritieme wapenwedloop tussen China en de VS (met India op de achtergrond). Deze ontwikkeling is verontrustend gezien het ontbreken van een regionale veiligheidsarchitectuur in dit gebied.

Een *tweede* "hot spot" waar sprake is van oplopende spanningen tussen grote mogendheden is Rusland en het Oosten van Europa. Het Russisch optreden tegen Oekraïne en de gewelddadige annexatie van de Krim heeft de verhoudingen tussen Rusland en in het bijzonder de EU-lidstaten en de VS (mede in NAVO-verband) op scherp gezet. Met zijn interventie heeft Rusland feitelijk aangegeven de uitgangspunten van de Europese veiligheidspolitieke orde zoals die onder andere in OVSE-kader zijn geformuleerd, niet langer te accepteren. Wat op termijn de Russische intenties zijn, is daarbij onduidelijk. Blijvende destabilisering van Oekraïne, meer territoriale annexatie of druk op Oostelijke EU- en NAVO-partners? Wel is duidelijk dat de verhoudingen tussen het Westen en Rusland ernstig onder druk staan, wat ook het overleg over mondiale kwesties ernstig belast.

Tot slot is er als *derde* "hot spot" de brede zone van instabiliteit, fragiliteit en conflict – als onderdeel van de "arch of instability"- die zich uitstrekt over de MENA-regio en sub-Sahara, West- en Oost-Afrika. Deze regio's worden op diverse plaatsen geteisterd door een explosieve mix van sektarisch en religieus geweld, extremisme en terrorisme en de teloorgang van legitiem overheidsgezag, met Irak, Syrië, Jemen, Libië en Nigeria als de landen die het meest bedreigd zijn. De conflicten zijn bovendien niet puur intern of lokaal, maar worden gevoed door externe partijen, waarbij vooral in het geval van Syrië, Irak, Libië en Jemen sprake is van een strijd om de regionale religieuze hegemonie tussen Iran enerzijds en Saoedi-Arabië en de Golfstaten aan de andere kant.

Vanuit de EU bezien betekent het voorgaande dat de Unie omringd is door – in de woorden van The Economist, "a ring of fire"[4] – een zone van instabiliteit met vanuit het Zuiden het risico van het overslaan van instabiliteit en conflicten naar het grondgebied van de EU in de vorm van terrorisme, extremisme en radicalisering, nog grotere vluchtelingenstromen, georganiseerde criminaliteit, etc. En vanuit het Oosten een intensivering van Russische agressie met inzet van alle middelen lopend van militaire middelen en steun aan separatisten tot en met economisch druk en propaganda, gericht op ondermijning en destabilisering van aangrenzende landen en de Europese Unie.

HET TOEKOMSTSCENARIO

In welke richting ontwikkelt de internationale orde zich? Gebruik makend van de scenario's zoals die ontwikkeld zijn in de Defensie Verkenningen komt de Clingendael Monitor 2015 in navolging van de eerdere edities van de Monitor tot de conclusie dat sprake is van een verdere verschuiving richting een multipolair scenario.[5] Binnen dit scenario is samenwerking mogelijk. Maar voor zover deze in de komende jaren plaatsvindt, zal zij waarschijnlijk sterk geconditioneerd worden door de relaties tussen de grote mogendheden, met – zoals al opgemerkt – de Amerikaans-Chinese verhouding als de belangrijkste as. In de Monitor 2015 wordt daarom gesproken over een versmelting van het multipolaire en het multilaterale scenario, waarbij sprake is van een mix van samenwerking en conflict. De grootste kans op samenwerking bestaat waarschijnlijk op het economische vlak, waar China een toenemend belang heeft bij een

[4] Charlemagne, "Europe's ring of fire; The European Union's neighbourhood is more troubled than ever", *The Economist* 20 september 2014.

[5] In dit project is indertijd een viertal scenario's geformuleerd die elk een denkbaar beeld van internationale verhoudingen schetsen. Als *eerste* een multilateraal scenario waarin staten georganiseerd met elkaar samenwerken. Als *tweede* een multipolair scenario, waarin de grote mogendheden domineren en dat door scherper wedijver wordt gekenmerkt. Als *derde* een scenario waarin de wereld fragmenteert en door conflict wordt beheerst. *Tot slot*, een netwerkscenario waarin niet staten domineren, maar een veelheid aan niet-statelijke actoren – al dan niet gewelddadig – de overhand heeft.

zekere orde.[6] Op veiligheidspolitiek terrein zal de bereidheid tot samenwerking sterk afhankelijk zijn van machtspolitieke overwegingen en alleen dan van de grond komen als de vitale belangen van de grote landen niet in het geding zijn. Voor effectieve samenwerking is hoe dan ook een voorwaarde dat de zich ontwikkelende internationale orde meer de opvattingen en posities van opkomende landen weerspiegelt. Daarmee zal deze orde minder westers en waarschijnlijk ook minder multilateraal verankerd zijn.

Bovenal laat de Monitor 2015 de kwetsbaarheid van de EU en daarmee van Nederland zien. Omringd als zij is door een zone van instabiliteit en fragiliteit wordt de Unie uitgedaagd in wat haar zwakke kant is: haar vermogen om als zelfstandige veiligheidspolitieke actor op te treden buiten de eigen grenzen. En dit dan in antwoord op een breed palet aan deels niet-traditionele dreigingen als migratie, terrorisme, cyber, etc. Ook Nederland is kwetsbaar voor deze dreigingen, die uiteindelijk alleen in samenwerking met partners zullen kunnen worden geneutraliseerd.[7]

[6] Daartegenover staat dat China juist op dit vlak nieuwe multilaterale instellingen lanceert, zoals de Aziatische Infrastructuur Investeringsbank. Op veiligheidspolitiek gebied wil China de rol van de VN versterken.

[7] Deze thematiek wordt verder uitgewerkt in twee Monitor verdiepingsstudies over respectievelijk afschrikking als instrument tegen nieuwe dreigingen en over de economische kwetsbaarheid van Nederland.

Versmelting van mulilaterale en multipolaire scenario's

Krijgsmacht – *koersvast in turbulente tijd*

Met het oog op de veranderende veiligheidssituatie en de hogere eisen die aan de krijgsmacht worden gesteld, zet het kabinet in op het verder versterken van de basisgereedheid. Dat hebben ministers Hennis-Plasschaert van Defensie en Koenders van Buitenlandse Zaken medio juni aan de Kamer laten weten.
De brief is een reactie op de september vorig jaar ingediende motie-Van der Staaij. Het kabinet wil de trendbreuk ten aanzien van Defensie voortzetten. De financiële consequenties voor de begroting van 2016 en de toekomstige financiering van de inzet van de krijgsmacht voor crisisbeheersingsoperaties worden op Prinsjesdag bekendgemaakt.
"Er moet rekening worden gehouden met een langdurige periode van spanningen en instabiliteit, dichtbij en ver weg". Internationale conflictbeslechting en preventie in de regio's om ons heen zijn in het belang van Nederland. Internationale crisissituaties kunnen immers een directe impact hebben op de nationale veiligheid.
"Gelet op de aard van de (internationale) veiligheidsproblematiek acht het kabinet versterking van de krijgsmacht noodzakelijk. Er is bovendien een actief buitenlandbeleid nodig, een actieve betrokkenheid bij de wereld om ons heen".
De internationale ontwikkelingen stellen structureel hogere eisen aan de gereedheid, paraatheid, verplaatsbaarheid en inzetbaarheid van militaire eenheden. Tevens is er extra capaciteit nodig voor

opleiding en training ter verbetering van de geoefendheid van operationele eenheden (inclusief de hogere geweldsniveaus).
Het kabinet acht een actief buitenland-, veiligheids- en defensiebeleid van wezenlijke betekenis voor onze strategische belangen, onze vrijheden en onze waarden. Een integrale benadering staat hierbij voorop. In dit verband wordt van Nederland, als lidstaat van de NAVO en de EU, verwacht dat het een bijdrage van betekenis levert, ook in militair opzicht.

(bron: Nieuwsbericht Ministerie van Defensie, 19 juni 2015)

Herziening Strategie Nationale Veiligheid

Marc Bökkerink en Marieke Oosthoek
NCTV, Ministerie van Veiligheid en Justitie

"Veiligheid ligt aan de basis van een samenleving waarin mensen zich vrij, vertrouwd en verbonden voelen. In ons dichtbevolkte land kunnen calamiteiten gemakkelijk voor een sneeuwbaleffect zorgen, met alle maatschappelijke gevolgen van dien. Garanties voor veiligheid zijn niet te geven. Maar met een goede analyse van mogelijke dreigingen, stevige afspraken vooraf en een heldere rolverdeling kunnen we veel leed en schade voorkomen."
Dit meldde de toenmalige Minister President Balkenende in het voorwoord van de Strategie Nationale Veiligheid die in 2007 het licht zag[1]. De strategie werd ontwikkeld om het kabinet beter in staat te stellen te bepalen welke dreigingen de nationale veiligheid in gevaar kunnen brengen en hoe daarop vervolgens te reageren. Klimaatverandering, mens- en dierziektes werden genoemd om te illustreren dat bedreigingen van de nationale veiligheid veranderen en steeds meer met elkaar verweven raken, waarmee het antwoord op deze bedreigingen niet langer van één ministerie of organisatie kan komen.

De nationale veiligheid is in het geding als nationale veiligheidsbelangen zodanig bedreigd worden dat er sprake is van – potentiële – maatschappelijke ontwrichting. Bij nationale veiligheidsbelangen gaat het om territoriale veiligheid, ecologische veiligheid, economische veiligheid, fysieke veiligheid en sociale en politieke stabiliteit.

Dat de complexiteit van onze samenleving niet is afgenomen blijkt wel uit scenario's die in de afgelopen jaren in het kader van de Strategie Nationale Veiligheid zijn geanalyseerd: cyberhacktivisme, schaarste aan mineralen en de geopolitieke context daarvan, wapenbeheersing falende staat, gewelddadige eenling, langdurige verstoring elektriciteit, grieppandemie en overstroming Lekdijk. Bij de dreigingen die in de scenario's beschreven werden, is steeds weer de vraag gesteld in welke mate de nationale veiligheid werd geraakt en of Nederland weerbaar is tegen die dreigingen en waar versterking nodig is.

Het kabinet meldde in mei aan de Tweede Kamer[2] dat in het afgelopen jaar op basis van alle opgedane ervaringen de balans is opgemaakt over de strategie. Geconstateerd is dat sturing en regie op nationale veiligheid onverminderd noodzakelijk is en dat de strategie Nationale Veiligheid een doorontwikkeling kan ondergaan om haar effectiviteit te blijven waarborgen.

[1] Strategie Nationale Veiligheid, april 2007: http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2007/05/14/strategie-nationale-veiligheid.html
[2] TK 2014-2015, 30821 nr. 23

NATIONALE VEILIGHEIDSPROFIEL

Het Nationaal Veiligheidsprofiel (NVP) komt in de plaats van de huidige nationale risicobeoordeling en wordt een vierjaarlijkse overkoepelende analyse van de belangrijkste (*all hazard*) risico's en dreigingen voor de nationale veiligheid, inclusief een overzicht van relevante technologische en maatschappelijke ontwikkelingen. Daarin zullen ook gezaghebbende internationale analyses en analyses op deelonderwerpen worden verwerkt. Het NVP zal in 2016 voor het eerst verschijnen. Bij het totstandkomingsproces van het NVP worden veiligheidsregio's en crisispartners betrokken. Het NVP en de regionale risicoprofielen zullen, daar waar relevant, op elkaar gaan aansluiten. Bevindingen uit dit profiel kunnen veiligheidsregio's aanleiding geven om hun regionale risicoprofiel te actualiseren of aan te scherpen.

STUREN OP TE VERSTERKEN CAPACITEITEN

Op basis van het Nationale Veiligheidsprofiel wordt een capaciteitenanalyse gedaan, waarin wordt bepaald of en in hoeverre Nederland voldoende is voorbereid op de dreigingen voor de nationale veiligheid die in het NVP zijn geïdentificeerd. Daarbij wordt, naast het Nationale Veiligheidsprofiel, gebruik gemaakt van eerdere capaciteitenanalyses, evaluaties uit crisisoefeningen en lessen uit incidenten in binnen- en buitenland. Ook technologieverkenningen vormen input voor het capaciteitenprogramma, wanneer zij leiden tot kansen om taken beter of goedkoper uit te voeren. Bij de analyse worden ook de capaciteiten van veiligheidsregio's en crisispartners betrokken. De ontwikkeling en implementatie van de te versterken capaciteiten worden opgenomen in een capaciteitenprogramma.
Uiteraard kunnen onverwachte of opkomende dreigingen aanleiding geven tot een tussentijdse risico- en capaciteitenanalyse.

Crisis.nl vernieuwd

De website crisis.nl is vernieuwd. De site geeft niet meer alleen informatie tijdens een noodsituatie, het is een platform waar mensen altijd terecht kunnen voor informatie over calamiteiten.

Crisis.nl is dé overheidswebsite waar je altijd terecht kunt voor betrouwbare informatie over rampen en crises.

Crisis.nl is opgericht om betrouwbare informatie te verspreiden tijdens een ramp. Alle overheden, zoals gemeentes en veiligheidsregio's, kunnen mensen via de site laten weten wat er aan de hand is en wat ze het beste kunnen doen. Sinds kort is de site niet alleen in te zetten tijdens een ramp. Op crisis.nl kunnen mensen altijd informatie vinden over hoe je je voorbereidt op een crisis, zoals aardbevingen en overstromingen.

Tijdens rampen geeft de site informatie over wat er aan de hand is en wat je op dat moment het beste kunt doen.

Dick Schoof, Nationaal Coördinator Terrorismebestrijding en Veiligheid: "Voorheen was crisis.nl meestal niet in gebruik. Hierdoor was de drempel hoog om de site in te zetten bij een crisis. Je gaat niet een hele website optuigen voor bijvoorbeeld een nieuwsbericht over een brand in de regio. Omdat er nu continu informatie op crisis.nl staat, is het plaatsen van een dergelijk bericht laagdrempeliger geworden. Daarnaast is crisis.nl robuust en kan de website hoge bezoekersaantallen aan. Het kan zo een goede aanvulling zijn op het totale pakket aan crisiscommunicatiemiddelen van onder andere lokale overheden."

Als er geen noodsituatie is, lees je op crisis.nl hoe je je kunt voorbereiden op een ramp. Bijvoorbeeld hoe je een noodpakket samenstelt of hoe je je mobiel kunt instellen voor NL-Alert. Schoof: "Als mensen goed zijn voorbereid, houden we de maatschappelijke impact van een ramp hopelijk zo klein mogelijk. Alle informatie over voorbereiding staat nu op crisis.nl."

Ook laat crisis.nl zien hoe je je voorbereidt op allerlei noodsituaties. Bijvoorbeeld door een goed noodpakket samen te stellen.

Verder staat er op crisis.nl meer crisis gerelateerd nieuws, zoals berichten over grote ontwrichtende gebeurtenissen in het land. Bijvoorbeeld de stroomstoring in februari. Daar stond een nieuwsbericht over op crisis.nl, dat verwees naar relevante instanties waar meer informatie te vinden was. Dat wil de NCTV met de nieuwe site vaker gaan doen. Schoof: "Zo zetten we crisis.nl op de kaart als een site waar iedereen terecht kan voor crisis gerelateerd nieuws. Crisiscommunicatie is essentieel tijdens een ramp of incident. Mensen willen weten wat er aan de hand is en wat zij moeten doen. Nu is crisis.nl een platform waar altijd informatie te vinden is: zowel tijdens een crisis als ter voorbereiding daarop".

Alle overheden, zoals gemeenten en veiligheidsregio's, kunnen crisis.nl inzetten om informatie te geven over een ramp of crisis.

Het Nieuws Gegijzeld: evaluatie veiligheidsincident bij NOS en NPO

Nico Kaptein, Abderrahman Kaouass en Marco Zannoni
COT Instituut voor Veiligheids- en Crisismanagement

AANLEIDING

Op donderdagavond 29 januari 2015 komt, kort voor het NOS Journaal van 20.00 uur, een man met ogenschijnlijk een vuurwapen het NOS-gebouw op het Media Park binnen en gijzelt een beveiliger. De man eist zendtijd en dreigt met het laten ontploffen van bommen op meerdere locaties en met een grootschalige cyberaanval. Even later overmeestert de politie de man en ontruimt gefaseerd de NOS- en NPO-gebouwen. Op de tv-zender NPO 1 vindt door de ontruiming enige tijd geen uitzending plaats, waarna om 21.05 uur het uitzenden wordt hervat vanuit de Haagse NOS-studio. Om 22.14 uur worden de gebouwen weer vrijgegeven. Door de gebeurtenissen worden NOS en NPO zelf intensief onderwerp van "nieuws". Uit nader onderzoek blijkt dat de man alleen handelt en dat het wapen geen vuurwapen is. Er zijn bij het doorzoeken door de politie geen explosieven aangetroffen.

LESSENONDERZOEK

NOS en NPO wilden leren van deze gebeurtenissen en hebben het COT Instituut voor Veiligheids- en Crisismanagement opdracht gegeven tot een evaluatie. Hierbij is geen sprake van "goed" of "fout". Bij iedere crisis zijn er uitdagingen en knelpunten, zijn er toevalligheden, is er emotie en gezond verstand, zijn er tegenvallers en onverwacht gunstiger ontwikkelingen. Dat maakt iedere crisis uniek. Het COT heeft zich gericht op het handelen van NOS en NPO en van relevante handelingen van anderen. De focus lag op beveiliging, continuïteitsmanagement en crisismanagement. In het onderzoek zijn interviews afgenomen en lessenbijeenkomsten georganiseerd. Omdat er bij NOS en NPO veel feitelijke vragen waren, hebben wij een gedetailleerde feitenreconstructie opgesteld.

LEERPUNTEN

NOS en NPO wilden met het onderzoek inzicht krijgen in leerpunten. Daarbij hoort ook de feitelijke constatering dat de situatie begint met een dreiger waarna beveiligers, NOS en NPO, politie en anderen moesten handelen. Hieronder de belangrijkste inzichten.

- De beveiliging werd geconfronteerd met een extreme en onzekere situatie waarin in zeer korte tijd keuzes moesten worden gemaakt. De beveiliging heeft bij de ontruiming rekening gehouden met de situatie door het ontruimingsalarm niet op alle etages af te laten gaan. Zo moest worden voorkomen dat collega's de gijzelnemer tegenkwamen. Ook heeft de beveiliging het stille alarm af laten gaan voor hulp. De initiële beveiligingsrespons is effectief, maar kende ook risico's voor de aanwezigen. De gijzelnemer is naar een andere studio gebracht dan hij vroeg. Zo zou de uitzending minder gevaar lopen. Wel was het daar drukker en waren er risico's voor collega's.

- De ontruiming is grotendeels goed verlopen, behoudens enkele knelpunten vanuit organisatiecultuur ("alles voor het nieuws") en menselijk gedrag ("niet alle medewerkers volgden de instructies"). Uiteindelijk werd de verbinding met de studio in Den Haag tot stand gebracht door een medewerker die was achtergebleven in het ontruimde gebouw. Dit toont de grote loyaliteit en de wens de uitzendingen te continueren, maar is ook gevaarlijk en daarmee niet acceptabel. Er is door de politie (begrijpelijkerwijs) geen rekening gehouden met kritische uitzendprocessen bij het ontruimen.

- Voor NOS en NPO heeft de duur van het niet uitzenden op NPO 1 veel impact gehad. Velen hebben hard gewerkt aan pogingen de uitzending te hervatten. Onze conclusie is dat een tijdelijke onderbreking onvermijdelijk was, maar dat dit minder lang had hoeven duren. Dit heeft vooral te maken met de (mis)communicatie, met technische mogelijkheden en met de tijdswinst die had kunnen worden gehaald met een eerder (kritiek) besluit over de te volgen strategie (wel of niet continueren uitzending en de wijze waarop). Radio-uitzendingen zijn doorgegaan: er was continuïteit van nieuwsvoorziening. Er is geen functionaliteit als landelijke rampenzender. De bestaande continuïteitsnorm van NOS en NPO is een eigen norm.

- Uit het onderzoek blijkt dat er grote betrokkenheid is bij medewerkers, directie en bestuurders. Tegelijk was er geen eenduidig beeld van de situatie en mede daardoor geen effectief crisismanagement bij NOS en NPO. Crisismanagement zou de verbindende schakel zijn tussen beveiliging, de continuïteit van uitzenden, het *breaking* nieuws, de impact op medewerkers en het zelf onderwerp zijn van nieuws. De crisisorganisatie is niet benut. Er is een groot deel van de avond geen effectief overleg met de politie tot stand gekomen. Dit is wel geprobeerd via het mediateam van de politie als vertrouwde partner en met de burgemeester. Er is wel operationeel maar geen strategisch contact tot stand gekomen. De burgemeester had geen nadere informatie. NOS en NPO wisten nu niet dat er na de gijzeling tijd nodig zou zijn voor nader onderzoek en dat er ontruimd zou worden. Dit terwijl een deel van de uitwijkmaatregelen was gestopt omdat de verwachting was dat na beëindigen van de gijzeling het NOS-gebouw toegankelijk zou zijn.

- Het belangrijkste leerpunt voor de voorbereiding is dat deze vooral fysieke calamiteiten, ernstige verstoringen en *breaking news* betrof. Hierbij lag de nadruk op technisch/operationele aspecten en niet op impact. NOS en NPO waren vooral voorbereid op BHV en continuïteitsmanagement, maar in mindere mate op crisismanagement voor een situatie waarin zij zelf werden getroffen.

AANBEVELINGEN

Onze belangrijkste aanbevelingen gaan over het versterken van de voorbereiding op crisismanagement, zowel binnen NOS en NPO als gezamenlijk. Ook adviseren wij NOS en NPO goed te kijken naar de bestaande technische en operationele planvorming en na te gaan of de impact van gebeurtenissen en maatregelen voldoende is meegenomen en of de beoogde uitvoering realistisch is. Deze les geldt zeker niet alleen voor NOS en NPO maar voor alle organisaties. Wat betreft beveiliging gaat het nu vooral om de eigen keuzes: wat is gegeven de risico's veilig genoeg? NOS en NPO hebben aangegeven aan de slag te gaan met de aanbevelingen. De belangrijkste breder toepasbare les is dat operationeel voorbereid zijn op bedrijfscontinuïteit (BCM) niet hetzelfde is als voorbereid zijn op uitzonderlijke situaties met een grote dynamiek en impact (crisismanagement).

Het volledige rapport kan worden gedownload op: http://over.nos.nl/nieuws/238/onderzoeksrapport-gijzeling-nos-gepresenteerd

VISIE OP CRISISMANAGEMENT ALS REFERENTIEKADER

Wij hebben onze door de jaren heen ontwikkelde visie op crisismanagement benut voor analyse en duiding. Een adequaat crisismanagement vergt het volgende.

- Denken vanuit de impact van een incident of crisis en de reactie hierop en niet alleen vanuit de directe bronbestrijding. Bijvoorbeeld de impact op direct betrokkenen, belangrijke stakeholders en/of de samenleving.
- Duidelijke strategische doelstellingen en uitgangspunten voor de aanpak van de crisis. Duidelijke doelstellingen geven richting aan de totale aanpak. Duidelijke uitgangspunten maken het mogelijk om richting te kiezen bij lastige vraagstukken of bij altijd aanwezige dilemma's. Bovendien is het mogelijk uitleg te geven bij keuzes en achteraf te verantwoorden waarom bepaalde maatregelen zijn getroffen.
- Oog voor de bijzondere aspecten van de specifieke crisis en situationeel bewustzijn van de omgeving waarin de crisis zich afspeelt om niet te vervallen in routinematige afhandeling die niet past bij de situatie van dat moment.
- Een integrale aanpak waarbij de maatregelen in samenhang worden bezien en waarbij maatregelen op het ene domein (zoals continuïteit of beveiliging) ook worden doordacht op bedoelde en onbedoelde implicaties voor een ander domein.
- Eenheid van inspanning zodat de inspanningen van alle betrokkenen bij de reactie op een incident of crisis optimaal samenkomen om de beoogde doelen te realiseren. Dit geldt voor alle interne partners maar ook voor externe partners.
- Een duidelijke organisatiestructuur die past bij wat de betreffende crisis van de organisatie vraagt. Dit vanuit een basis die is voorbereid en die flexibel is ingevuld/aangepast op basis van de werkelijke situatie die zich voordoet.
- Leiderschap waarbij de leider een wenkend perspectief biedt "door de crisis heen". Vanuit kalmte en rust wordt met vastberadenheid richting gekozen en gewerkt aan een slagvaardige uitvoering.

Nepal: De ramp van de aardbeving en de ramp van de hulp!

Naar aanleiding van de tsunamiramp in 2004 heb ik ooit een boekhoofdstuk geschreven onder de titel "*Principles ignored and lessons unlearned*".[1] Hierin bekritiseerde ik de aanpak van de toenmalige ramp omdat principes voor noodhulpverlening en lessen opgedaan tijdens eerdere rampen - zoals neergelegd in diverse internationale verklaringen en actieplannen - waren genegeerd en de hulp daardoor minder goed de behoeftigen wist te bereiken dan gewenst was. Ondanks de inzet van talloze individuele hulpverleners en organisaties, is het onthutsend om te zien hoeveel er weer misgaat bij de hulpverlening aan Nepal en hoeveel van deze problemen *man-made* zijn, ondanks de verwoestende kracht van de aardbeving zelf.

■ ***Georg Frerks***
Hoogleraar Conflictstudies Universiteit van Utrecht en hoogleraar Internationale Veiligheidsstudies Nederlandse Defensieacademie. Tot medio 2014 tevens hoogleraar Rampenstudies aan de Universiteit van Wageningen.

DE GHORKA AARDBEVING IN NEPAL

Op 25 april jl. werd Nepal opgeschrikt door de *Ghorka* aardbeving met een grootte van 7.8 op de schaal van Richter. De aardbeving zaaide dood en verderf en werd twee weken later gevolgd door een tweede aardbeving van 7.3 op de schaal van Richter en tal van kleinere naschokken, modderstromen en lawines. Het gevaar op landverschuivingen neemt intussen alleen maar toe met de naderende moessonregens. In totaal verloren bijna 9.000 personen het leven, raakten dubbel zoveel mensen gewond, naast nog een groot aantal vermisten. Meer dan 70.000 huizen werden vernietigd en een half miljoen in min of meerdere mate beschadigd. Honderdduizenden mensen bivakkeren in de open lucht. Ook werden vele unieke UNESCO werelderfgoed locaties getroffen. In 1833 en 1934 werd Nepal ook al getroffen door zware aardbevingen. Nepal ligt op het punt waar de Indiase en Euraziatische tektonische platen met elkaar botsen en de vrijkomende energie wordt omgezet in aardbevingen. Door de seismische gevoeligheid van Nepal kan men eigenlijk dus gewoon weer wachten tot de volgende aardbeving zich aandient.

FALENDE PREVENTIE

Dit inzicht had in 2008 geleid tot de formulering van een *National Strategy for Disaster Risk Management* met de hulp van het Ontwikkelingsprogramma van de Verenigde Naties (VN) en verschillende donorlanden. Het was de bedoeling om kwetsbare gebouwen via een programma van "retrofitting" aardbevingsbestendig te maken. Door bevolkingsgroei en snelle urbanisatie waren er echter overal betonnen gebouwen met meerdere verdiepingen verrezen die in het geheel niet aan de bouwvoorschriften voldeden, laat staan aardbevingsbestendig waren gebouwd. Hierop was praktisch geen enkele controle of kon deze gemakkelijk omzeild worden al dan niet via omkoping. Ook was het de bedoeling de responscapaciteit van de overheid bij rampen te verhogen en de bevolking en de overheidsdiensten bewust te maken van rampenpreventie. Helaas is de uitvoering van dit programma tot stilstand gekomen door het wanbeleid van de regering van Nepal, die de laatste jaren ernstig was verdeeld, in een bestuurlijke impasse was beland en bijgevolg weinig daadkracht vertoonde.

STRUCTURELE PROBLEMEN

Ook behoort Nepal tot de relatief armste landen ter wereld met een gemiddeld jaarinkomen van ongeveer US$ 700 per hoofd van de bevolking. Bovendien is het voor bijna 10% van het bruto nationaal inkomen afhankelijk van de toerismesector die thans volledig is lamgelegd door schade aan monumenten, hotels, trekking routes en dergelijke. Het land heeft weinig capaciteit er zelf boven op te komen. Het wordt daarnaast ook nog eens geteisterd door ernstige corruptie. Een rapport van de *Economist* uit 2011 documenteerde een wijdverbreid misbruik van hulpgelden die tot wel 90% werden opgeslokt door georganiseerde misdaad en corrupte ambtenaren, leidend tot een massieve verspilling binnen ontwikkelingsprojecten.[2] Op dit moment is Nepal volledig afhankelijk van buitenlandse donoren voor de aanpak van de ramp. Er is niet alleen veel geld nodig voor de eerste levensbehoeften van de getroffenen, maar ook voor de wederopbouw van het land. Voorlopige schattingen lopen uiteen tussen 5 en 10 miljard dollar.

PROBLEMEN BIJ DE HULPVERLENING

Er is gelukkig veel hulp op gang gekomen voor de getroffenen in Nepal door internationale organisaties van de VN, bilaterale donoren, niet-gouvernementele organisaties en particulieren. Ook hebben de buurlanden veel hulp gegeven, zoals India, Pakistan en China. De hulpverlening wordt begrijpelijkerwijs bemoeilijkt door gebruikelijke problemen bij rampen als gebrekkige communicatie en transportmiddelen, het uitvallen van elektriciteit etc. Daar zijn

[1] G. Frerks, "Principles ignored and lessons unlearned, a disaster studies perspective on the tsunami experience in Sri Lanka", in: D.B. McGilvray and M.R. Gamburd (eds.) *Tsunami Recovery in Sri Lanka. Ethnic and regional dimensions*, London and New York: Routledge, 2010, 143-162.

[2] O. Crowcroft, 'Nepal earthquake: Corruption and shattered tourism industry jeopardise long-term recovery', *International Business Times*, April 27, 2015.

hulpverleners wel aan gewend, maar intussen is er onder de Westerse donoren en hulpverleners veel onrust ontstaan over een geheel ander probleem. De regering heeft namelijk een missive doen uitgaan waarin geëist wordt dat alle hulpgelden via het *Prime Ministers Disaster Relief Fund* worden geleid. Er bestaat onder internationale actoren echter in het geheel geen vertrouwen dat dit geld efficiënt wordt besteed, niet naar politieke protegés wordt gekanaliseerd of misschien wel in privézakken verdwijnt. De overheid wordt beschuldigd van een monopolisering van de hulp, maar zegt op haar beurt dat dit juist nodig is om de transparantie, verantwoording en coördinatie van de hulp te bevorderen. Deze kwestie heeft er volgens waarnemers toe geleid dat de broodnodige hulp onnodige vertraging heeft opgelopen wegens toegenomen wantrouwen. *Amnesty International* heeft de overheid beschuldigd van discriminatie op basis van *gender*, kaste en etnische achtergrond. Ook werd gezegd dat de overheid politieke spelletjes speelt, bijvoorbeeld door hulp van Britse Chinook helikopters te weigeren vanwege de vervolging in het Verenigd Koninkrijk van een Nepalese kolonel in verband met mensenrechtenschendingen in de periode 1996-2006.

Inzet USAR.NL bij de aardbevingsramp Nepal

COÖRDINATIE

Ondanks de eigen pretenties bleek de overheid in de praktijk niet in staat de eigen bevolking afdoende te helpen of de hulp adequaat te coördineren. De eerste dagen na de ramp werden gekenmerkt door een complete chaos en de overheid was niet in staat leiding te geven aan de binnenkomende hulp en hulpverleners en hun activiteiten goed op elkaar af te stemmen. Vele slachtoffers hebben dagenlang tevergeefs op hulp zitten wachten. De geringe daadkracht van de Nepalese overheid leidde tot wanhoop van de vele lokale en buitenlandse hulpverleners die klaar stonden om te helpen, maar geen vergunning kregen te beginnen. Ook bleken goederen aan de grens te worden opgehouden. Gelukkig zijn andere organisaties in het gat gesprongen dat ontstond. Zo heeft het Nederlandse *Urban Search and Rescue Team* USAR.NL zich niet alleen verdienstelijk gemaakt door naar overlevenden te zoeken, lichamen te bergen, gewonden te verzorgen en hulp te distribueren, maar vooral ook de coördinatie van de ruim zestig internationale reddingsteams ter hand genomen. Er werd een speciale tent opgezet als centraal meldingspunt voor de internationale reddingsteams zodat de werkzaamheden structureel kon worden aangepakt en doublures of witte vlekken in de reddingsoperaties konden worden voorkomen. Zowel de Nepalese overheid als de VN hebben hun waardering uitgesproken voor deze belangrijke coördinerende bijdrage door het Nederlandse reddingsteam.

CONCLUSIE

In feite is de situatie waarin Nepal zich bevindt als gevolg van de aardbeving slechts een uitvergroting van de normale problemen waar het land al onder gebukt gaat. Ontwikkelingshulp kwam ook al eerder niet dáár aan waar het voor bedoeld was, waardoor hele groepen kwetsbaar voor rampen werden gemaakt. De regering en het leger werkten al langere tijd alleen al voor zichzelf en niet voor diegenen in het land die het 't hardste nodig hadden. De gepoogde opbouw van capaciteit om rampen adequaat het hoofd te bieden en te coördineren was gestrand in de overheidsbureaucratie en de politieke wanorde van het land. Het is triest te constateren dat ook de donor gemeenschap dit te lang op zijn beloop heeft gelaten. De vele miljoenen die in Nepal zijn geïnvesteerd, hebben de allerarmsten nauwelijks bereikt, terwijl er door de donoren niet hard genoeg aan de bel is getrokken en we nu met machthebbers zitten die hiermee altijd maar zijn weggekomen.

Hoe kan een herhaling van deze malaise thans voorkomen worden? Er ligt een grote uitdaging de getroffenen te helpen, maar tevens om te zorgen dat de hulp niet verdampt of terecht komt op plekken waar die niet nodig is, zoals bij de lokale elites en partijbonzen. De internationale gemeenschap zal nu wel het achterste van zijn tong moeten laten zien en samen met de bevolking moeten eisen dat de overheid zich behoorlijk en fatsoenlijk gedraagt in het aangezicht van zoveel leed en dat de hulp goed en eerlijk wordt gecoördineerd en verdeeld.

10-JARIG LOCC VERSTERKT FACILITERENDE ROL

Verbinden van kennis en expertise is onze kracht

Rob Jastrzebski

Ira Helsloot met de zaal in debat over "coördinatie".

Al tien jaar speelt het Landelijk Operationeel Coördinatie Centrum een voorname rol in de nationale operationele crisisbeheersing. Tien woelige jaren, waarin de maatschappij en het landschap van nationale veiligheid drastisch zijn veranderd. Die dynamiek zal de komende tien jaar alleen maar toenemen en daarom is het tijd voor herbezinning op de rol van het LOCC in de nationale crisisstructuur. De jubilaris organiseerde op 10 juni een themamiddag om samen met nationale en regionale crisispartners vooruit te kijken naar de uitdagingen van morgen. Operationele crisisbeheersing 10 jaar vooruit; waar staan we in 2025?

De wapenfeiten spreken klare taal; in de voorbije tien jaar heeft het LOCC zijn coördinerende en faciliterende rol waar gemaakt. Ongeveer 200 bovenregionale, nationale en internationale verzoeken om capaciteit, kennis en expertise handelt het LOCC jaarlijks af. Van kleinschalige bilaterale bijstandsverzoeken tot complexe internationale operaties. Met als uitschieters de brand bij Chemiepack in Moerdijk, de crash van Turkish Airlines, de ingewikkelde repatriëring van de slachtoffers van de MH17-ramp en grote evenementen als de NSS-top in Den Haag en de inhuldiging van Koning Willem-Alexander.

VERANDEREND CRISISLANDSCHAP

Geen twijfel over het nut van het LOCC in het stelsel van de nationale crisisbeheersing dus. Maar toch, veranderingen in het speelveld van nationale veiligheid vragen om een kritische herbezinning op het functioneren van de nationale structuur voor crisisbeheersing en crisisbesluitvorming. Want de dreigingen van morgen zijn anders dan de dreigingen van gisteren. Crisisscenario's worden complexer en hebben grotere impact op de moderne netwerksamenleving. Ook het aantal partners dat bij crises een rol speelt, groeit. Met die ontwikkelingen als stimulans moet de nationale crisisbeheersingsstructuur – en als onderdeel daarvan ook het LOCC – toekomstproof worden gemaakt, kondigde Nationaal Coördinator Terrorismebestrijding en Veiligheid Dick Schoof tijdens de themamiddag aan.

"Om daar invulling aan te geven, is binnen en buiten de NCTV een groot aantal verbetertrajecten gaande. De nationale crisisbeheersingsstructuur moet verder worden geoptimaliseerd. In die structuur zoeken we naar een passende invulling van de rol van het LOCC als verbindingsplatform voor capaciteit, kennis en kunde. Passend bij de inrichting van het veiligheidsdomein waar in het afgelopen decennium:

- de veiligheidsregio's hun intrede hebben gedaan;
- de brandweer is geregionaliseerd;
- de nationale politie is gerealiseerd;
- de volgende fase van versterking van de civiel-militaire samenwerking van start is gegaan.

De volgende grote operatie – de bouw van één landelijke meldkamerorganisatie – is inmiddels ook in volle gang."

URGENTIE

Schoof kondigde aan dat de experimenten met een Landelijke Operationele Staf voor bovenregionale coördinatie geen vervolg zullen krijgen. Een dergelijke staf past niet in de Nederlandse crisisstructuur. Voor de gewenste advisering bij bovenregionale crisissituaties moet een nieuwe invulling worden gevonden. Volgens Ira Helsloot, hoogleraar Besturen van Veiligheid, moet in ieder geval goed worden nagedacht over wat het fenomeen "coördinatie" nu precies behelst. "Want niemand wil graag gecoördineerd worden", stelt Helsloot vast. "Een aanname is dat zich op een dag een worst case crisisscenario kan voordoen, waarbij echte operationele coördinatie met een staf op nationaal niveau noodzakelijk is, omdat de schaal en complexiteit de crisisorganisaties van de veiligheidsregio's te boven gaat. Maar tot dusver voelt de samenleving de urgentie voor die krachtige landelijke operationele regie nog niet."
Belangrijker dan coördineren is volgens Helsloot het pretentieloos faciliteren van de ketenpartners en maatschappelijke netwerken met capaciteit en expertise. Zo kunnen veiligheidsregio's, departementen, lagere overheden en vitale sectoren goed invulling geven aan hun rol in het crisismanagement. Zij hebben vooral behoefte aan een nationaal overheidsniveau dat hen "ontzorgt" met het regelen van capaciteit, kennis en kunde. Helsloot onderschrijft het belang van het LOCC daarin: "Als het LOCC er nog niet was geweest, dan had het zeker uitgevonden moeten worden!"

VERBINDEN EN FACILITEREN

Verbinden, faciliteren en ontzorgen zijn ook de kernwoorden in de positie die hoofd LOCC Guus Appels voor zijn organisatie ziet, als hij tien jaar vooruit kijkt. "De term coördineren dekt eigenlijk de lading niet goed. Want wij coördineren geen acties, maar capaciteit. Alleen in de nationale crisisbeheersingsstructuur hebben we ook een daadwerkelijke coördinatiefunctie. Maar het grootste deel van ons werk betreft ondersteuning aan veiligheidsregio's bij opschalings- en bijstandsvraagstukken. In het verbinden van mensen en organisaties met kennis en expertise zit onze kracht. Dat werd duidelijk tijdens de

vogelgriepuitbraak afgelopen november. Hoewel er formeel geen coördinerende taak voor het LOCC lag, hebben we in een vroeg stadium het initiatief genomen om relevante partijen bij elkaar aan tafel te brengen, zoals de NVWA, de veterinaire sector, de veiligheidsregio's en experts op het gebied van volksgezondheid. Met die aanpak konden de partners bovenregionaal en over organisatiegrenzen heen breed anticiperen en scenario's voorbereiden voor als de besmetting zich zou uitbreiden."
Deze verbindende rol werd volgens Appels door alle betrokken organisaties zeer gewaardeerd en daarin wil hij de komende jaren dan ook verder investeren. "In de eerste tien jaar van ons bestaan zijn we vooral actief geweest als coördinerende en faciliterende spil in de responsfase. Geleidelijk verschuift onze rol ook naar de preparatiefase en het faciliteren van het netwerk van nationale en regionale crisispartners, ook in de multidisciplinaire voorbereiding op potentiële risico's en crises."

VITALE INFRASTRUCTUUR

Die sterkere rol als verbinder van netwerken kan goed uitpakken voor de vitale sectoren, die als private partijen ook een stevige rol hebben te spelen in het voorkomen en oplossen van crises en grote maatschappelijke verstoringen. Stef Nieuwland, manager Continuïteit bij elektriciteitsnetbeheerder Alliander ziet er wel heil in: "De bovenregionaal en landelijk opererende netwerkbedrijven en andere vitale ondernemingen hebben in de preparatie- en responsfase grote behoefte aan een verbindende schakel die partijen bij elkaar kan brengen om acties af te stemmen. De vitale sectoren en de overheid hebben beide een stevige crisisorganisatie, maar synergie tussen beide werelden tijdens een bovenregionale calamiteit ontbreekt nog. Tijdens de grote stroomstoring in Noord-Holland in maart bleek het bijna onmogelijk om met vijf regio's afzonderlijk afspraken te maken. De bovenregionale coördinatie raakte in een impasse, naar mijn mening omdat de veiligheidsregio's het ingewikkeld vinden om één regio de regie te laten nemen. In dat licht zie ik de rol van het LOCC als verbindende partij op bovenregionaal operationeel niveau als onmisbaar."

WEERBARE SAMENLEVING

Dat is ook de visie van Hugo Backx, directeur van GGD GHOR Nederland. Als koepeldirecteur in de witte keten ziet hij veel raakvlakken tussen de publieke gezondheid en het veiligheidsdomein. Zoals de voorbereiding op uitbraken van infectieziekten en pandemieën en effecten van rampen en crises op de zorgketen. "Een vraagstuk dat ons in toenemende mate zorgen baart, is het feit dat door het veranderende zorgstelsel steeds meer mensen met een zorgbehoefte zelfstandig blijven wonen. Als GGD GHOR willen we grip krijgen op dit vraagstuk en handelingsperspectieven ontwikkelen voor deze snel groeiende populatie verminderd zelfredzamen in de samenleving. Ik zou het LOCC willen vragen ons daarbij te helpen in de preparatiefase. Het LOCC heeft al veel praktijkkennis en ervaring opgebouwd met grote crisisbeheersingsvraagstukken, scenariovoorbereiding en het coördineren van ondersteuningsoperaties. Die kennis kan ook voor ons werkterrein van grote waarde zijn."
Boeiende perspectieven voor een vernieuwd LOCC in een weerbare netwerksamenleving, waar de rijksoverheid verbindt en faciliteert; de uitdaging voor het LOCC in 2025 staat. NCTV Dick Schoof ziet ook in het komende decennium een belangrijke schakelfunctie voor het LOCC weggelegd in het stelsel van crisisbeheersing, dat flink op de schop gaat. In de migratie naar een LOCC nieuwe stijl is er volgens Schoof ook aandacht voor de positionering van het LOCC in termen van beheer en aansturing. Want de aansturing ligt nu rechtstreeks bij het ministerie van Veiligheid en Justitie, terwijl het LOCC eigenlijk voor en van de regio's en de kolommen is. Dáár zit de capaciteit en expertise die het LOCC bemenst. Een waarborg voor vakmanschap gestoeld op operationele ervaring van de medewerkers. Dat zal ook in de toekomst zo blijven.

Artistieke interpretatie tien jaar operationele crisisbeheersing. Met dank aan wandverslag.nl

MONSTERTRUCKONGEVAL HAAKSBERGEN

Vergunningverlening als veiligheidskritisch proces

De evenementenvergunning is een belangrijk instrument waarmee de overheid de veiligheid van evenementen kan beïnvloeden. Dat maakt het verlenen van die vergunning tot een veiligheidskritisch proces. Wat betekent dat voor de inrichting en uitvoering van dat proces? De wijze waarop de vergunning voor het evenement AutoMotorSportief in Haaksbergen is verleend, leert enkele waardevolle lessen, zoals onderzoek door de Onderzoeksraad voor Veiligheid uitwijst.[1]

Dr. N. (Niels) Smit
Projectleider Onderzoeksraad voor Veiligheid

Op zondagmiddag 28 september 2014 vond in de gemeente Haaksbergen de afsluiting plaats van het jaarlijkse evenement AutoMotorSportief. Op het programma stond onder meer een demonstratie met een monstertruck van 1500pk, die over enkele autowrakken heen zou rijden. De demonstratie vond plaats op een parkeerterrein van 51 bij 66 meter dat was afgezet met dranghekken. Het publiek kon aan alle zijden plaatsnemen om niets van het spektakel te hoeven missen. Halverwege de demonstratie reed de monstertruck plotseling in op het publiek, waarbij drie doden en 28 gewonden vielen.

In Nederland worden jaarlijks duizenden evenementen georganiseerd, die miljoenen bezoekers trekken. Al deze bezoekers gaan er vanuit dat zij niet worden blootgesteld aan gevaar, zolang ze zich zelf verantwoordelijk gedragen. Dat is een terechte, en doorgaans ook juiste, veronderstelling. De Onderzoeksraad voor Veiligheid vindt dat inwoners van Nederland zich beschermd mogen weten tegen gevaren waartegen zij zich niet zelf kunnen wapenen.
Bij evenementen moeten in de eerste plaats de organisator van het evenement en partijen die in zijn opdracht handelen, deze bescherming bieden. Zij moeten de risico's in beeld brengen die met hun activiteiten samenhangen en daartegen passende maatregelen treffen. Maar ook de overheid heeft een belangrijke rol. Die moet erop toezien dat de wijze waarop de organisator zijn risico's beheerst de openbare veiligheid in voldoende mate waarborgt. De wetgever heeft voor deze taak in artikel 174 Gemeentewet de burgemeester als bevoegd gezag aangewezen.

De evenementenvergunning is één van de instrumenten die de burgemeester hiervoor tot zijn beschikking heeft. Door aan de vergunning voorschriften en beperkingen te verbinden waaraan de organisator zich moet houden, kan de burgemeester bevorderen dat de organisator zijn risico's afdoende beheerst. Wanneer de burgemeester verzuimt om aan de evenementenvergunning voorschriften en beperkingen te verbinden die passen bij de risico's die met het evenement samenhangen en ook overigens geen invulling geeft aan zijn toezichtstaak bij evenementen, laat hij de beheersing van die risico's, en daarmee de zorg voor de openbare veiligheid tijdens het evenement, in feite geheel over aan de organisator. In die zin is het verlenen van een evenementenvergunning, bezien vanuit het belang van de openbare veiligheid waarvoor de gemeente hoort te waken, een veiligheidskritisch proces.

In de vergunning voor AutoMotorSportief 2014 had de gemeente Haaksbergen geen voorschriften en beperkingen opgenomen die samenhangen met het rijden met een monstertruck op een klein terrein. De vergunning schreef slechts het gebruik van dranghekken voor om het publiek op afstand te houden. Hoewel daarmee het risico wordt beheerst dat bezoekers zich op het evenemententerrein begeven, bieden dranghekken geen enkele bescherming in situaties

Evenementen in Nederland. Bron: Respons

[1] Het volledige rapport is te downloaden via www.onderzoeksraad.nl.

waarin de monstertruck van het voorgenomen parcours af raakt. De Onderzoeksraad concludeert om die reden dat de evenementenvergunning nauwelijks heeft bijgedragen aan een veilig verloop van de demonstratie met de monstertruck.

De onvolkomenheden in de evenementenvergunning werpen de vraag op in hoeverre de verlening van evenementenvergunningen in de gemeente Haaksbergen functioneert als een veiligheidskritisch proces. Het onderzoek van de Onderzoeksraad wijst uit dat daarop het nodige valt aan te merken. In plaats van de aanvrager kritisch te bevragen op zijn plannen en zich er zo van te overtuigen dat deze de risico's in beeld had en adequaat beheerste, verleenden de ambtenaren de vergunning zonder kennis te nemen van de specifieke inhoud van het evenement en daaraan passende voorschriften te verbinden. In plaats daarvan namen zij de voorschriften uit de vergunning van het voorgaande jaar over. Daarbij werd de aanvraag in behandeling genomen hoewel deze slechts elf dagen voor het evenement werd ingediend en diverse bescheiden, waaronder situatietekeningen en een draaiboek, ontbraken. Bovendien werd het evenement aanvankelijk verkeerd geclassificeerd in de regionale risicoclassificatie en was een latere herclassificatie, die veel hoger uitviel, geen aanleiding om de toen al verstrekte vergunning nog eens kritisch tegen het licht te houden.

Het lijkt er sterk op dat de ambtenaren zich bij het behandelen van de aanvraag hebben laten leiden door hun perceptie van het evenement, in plaats van te kijken naar de feitelijke risico's van de editie in 2014. Die perceptie was gunstig: AutoMotorSportief werd in Haaksbergen algemeen gezien als een gezellig, "braderie-achtig" gezinsevenement dat al jaren zonder problemen plaatsvond en georganiseerd werd door een betrouwbare partij. Dat het evenement zich in de loop der jaren had ontwikkeld en door programmering van steeds spectaculairder vermaak steeds meer risico's kende, was niemand opgevallen.

De constatering dat de betrokken ambtenaren fouten hebben gemaakt, is echter maar de helft van het verhaal. Fouten maken is menselijk en ook vergunningverleners zijn niet onfeilbaar. Zorgwekkender vindt de Onderzoeksraad voor Veiligheid het dan ook dat de wijze waarop in Haaksbergen een evenementenvergunning tot stand komt, in feite geheel wordt overgelaten aan de met die taak belaste ambtenaren. Zowel het management van de gemeentelijke organisatie als de – inmiddels teruggetreden – burgemeester onder wiens mandaat de vergunning wordt afgegeven, wijzen in dit verband op het vertrouwen dat zij stellen in de professionaliteit van de ambtenaren. Op zich lijkt dat een behartenswaardige instelling, waar menig leidinggevende iets van kan leren. Echter, vertrouwen krijgt trekken van desinteresse wanneer de professionele ruimte van een medewerker zo groot wordt gemaakt dat hij op zichzelf wordt teruggeworpen. Wanneer een professional geen duidelijke kaders meekrijgt waarbinnen hij zijn taak moet uitvoeren, hij niet uitgedaagd wordt om op zijn taakuitoefening te reflecteren en het aan hemzelf wordt overgelaten om te signaleren in hoeverre zijn kennis en vaardigheden nog toereikend zijn om zijn taak naar behoren uit te voeren, dan wordt de kwaliteit van zijn taakuitoefening afhankelijk van toevalligheden. Van een beheerst proces is dan geen sprake meer.

Om te voorkomen dat de hierboven geschetste ontwikkeling zich voordoet, is het van belang om vergunningverlening voor evenementen zodanig in te richten en aan te sturen dat de betrokken functionarissen gestimuleerd worden om elke aanvraag met gepaste waakzaamheid te behandelen, telkens alert op mogelijke onbeheerste risico's die de openbare veiligheid in het geding kunnen brengen. Bijvoorbeeld de theorie van Weick en Sutcliffe (2007) over hoog betrouwbaar organiseren biedt hiervoor handvatten.[2] Te denken valt aan nadruk op uitgangspunten in plaats van regels, investeringen in de kennis en vaardigheden van de ambtenaren en een zodanige inrichting van het proces dat evaluatie en intercollegiale toetsing vanzelfsprekend is. Hiervoor is voortdurende, zichtbare bestuurlijke aandacht van de burgemeester voor dit belangrijke werk een essentiële voorwaarde.

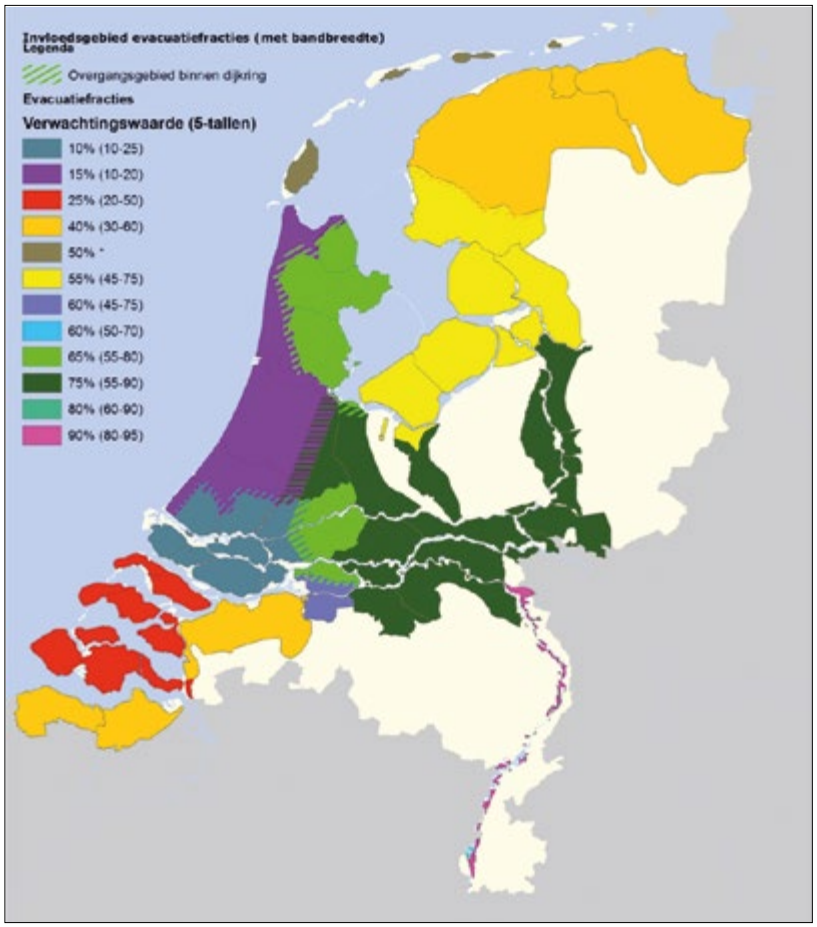
De Onderzoeksraad heeft de indruk dat er niet veel gemeenten zijn waarin de vergunningverlening voor evenementen functioneert volgens de uitgangspunten van hoog betrouwbaar organiseren. Vooral gemeenten waar weinig evenementen plaatsvinden, zijn kwetsbaar. Daar heeft deze vorm van vergunningverlening vaak de karaktertrekken van een administratief proces, waarin procedurele zorgvuldigheid en eenduidigheid belangrijker zijn dan inhoudelijke scherpte. Juist voor die gemeenten moet het ongeval in Haaksbergen een aanleiding vormen om zich te beraden. De burgemeesters moeten hierin, als hoeders van de openbare veiligheid, het voortouw nemen.

[2] K.E. Weick & K.M. Sutcliffe, *Managing the Unexpected: Resilient Performance in an Age of Uncertainty*. 2nd ed. John Wiley & Sons, 2007.

Randvoorwaarden voor verticaal evacueren

Wanneer een overstroming dreigt, is het niet altijd mogelijk iedereen preventief uit het bedreigde gebied te evacueren. Een alternatief is om mensen op te roepen verticaal te evacueren naar een droge verdieping thuis of elders in het bedreigde gebied zodat ze niet “onderweg” worden getroffen als ze het meest kwetsbaar zijn. De keerzijde is dat verticaal geëvacueerden enkele dagen tot een week in het rampgebied moeten overleven, terwijl veel voorzieningen (gas/water/elektriciteit, telefonie, infrastructuur) zijn uitgevallen. In het onderzoek is gekeken naar mogelijke randvoorwaarden die gesteld kunnen worden voor verticaal evacueren.

■ **Bas Kolen en Teun Terpstra**
HKV
■ **Maureen Turina**
WODC



De vraag werpt zich op of de overheid aanvullende eisen moet stellen aan zichzelf of andere partijen, om verticale evacuatie bij overstromingen (beter) mogelijk te maken? Het gaat hierbij om reductie van het slachtofferrisico als de leefbaarheid te vergroten. HKV lijn in water en TNO hebben in opdracht van WODC onderzoek hiernaar verricht. Het onderzoek omvat twee expertsessies omtrent de thema’s “fysieke infrastructuur” en “gedrag van mensen”. Daarnaast zijn case studies verricht in Dordrecht en Mastenbroek (een polder in de IJssel-Vechtdelta).

De noodzaak voor het stellen van randvoorwaarden kan benaderd worden vanuit een perspectief van het verkleinen van de gevolgen, hiervoor bestaan echter geen concrete criteria om maatregelen te ontwerpen. Een ander perspectief is vanuit een acceptabel risico. Recent zijn in het Deltaprogramma nieuwe normen voor waterkeringen bepaald waarbij voor iedere Nederland een minimale basisveiligheid is gegarandeerd. In feite wordt hiermee invulling gegeven aan het acceptabel risico, al verwacht de bevolking ook bij een dreiging passende maatregelen. Beide perspectieven spelen dan ook een rol. Verder spelen overwegingen als kosten, de uitvoerbaarheid, de omvang, onzekerheid door kennis- en ervaringsgebrek en de verdere acceptatie van slachtoffers een rol.

De belangrijkste voorwaarde voor verticale evacuatie is dat er vluchtplaatsen (hoog en droog) in de buurt beschikbaar zijn. Als de overstroming stabiliseert, zal men het gebied alsnog verlaten. Verticaal evacueren is bedoeld als tijdelijke maatregel om de overlevingskansen te vergroten. Onderzoek laat zien dat 60 tot 90% van de mensen zichzelf redt of met hulp van medeburgers. Uit de case studies blijkt dat veel huizen en andere gebouwen nu al een droge verdieping bieden, een beperkt aantal buurten heeft relatief weinig mogelijke vluchtplekken.

Nuts- en ICT-voorzieningen vallen uit in het overstroomd gebied of zijn reeds afgeschakeld door de beheerder vanwege schadebeperking, overbelasting of om keteneffecten te voorkomen. Het preventief afschakelen van nuts- en ICT-voorzieningen heeft een negatief effect op het handelingsperspectief in de dreigingsfase. Zowel de preventieve als verticale evacuatie zal minder goed kunnen worden voorbereid. Hierbij dient opgemerkt te worden dat evacuaties naar verwachting minstens 5x vaker voorkomen dan overstromingen. Er zal dus relatief vaak “onnodig” afgeschakeld worden wat de vraag oproept wat maatschappelijk het meest verstandig is.

De verantwoordelijkheden van burgers liggen in het verlengde van het dagelijks leven zoals het hebben van voldoende voedsel, drinken, medicijnen en de zorg voor de eigen veiligheid. Wat "voldoende" is om te overleven hangt sterkt af van de persoon en de duur van een verticale evacuatie. Onderzoek laat zien dat de zelfredzaamheid van burgers vaak wordt onderschat.

Nederlandse studies tonen aan dat mensen verticale evacuatie als een realistisch handelingsperspectief zien en dat hun percepties door middel van communicatie kunnen worden beïnvloedt. Mensen dienen bekend te zijn met de optie van verticaal evacueren en te weten dat preventief evacueren soms juist gevaarlijker is. Voor het benutten van verticale evacuatie is specifieke risico- en crisiscommunicatie dus een randvoorwaarde. Naast een goede informatievoorziening zijn de belangrijkste randvoorwaarden de gezondheid van de mensen, de sociale netwerken waarin mensen functioneren en algemene vaardigheden zoals EHBO. Het versterken hiervan is niet alleen van belang voor evacuaties, maar draagt ook bij aan de zelfredzaamheid in het algemeen.

Het onderzoek heeft geleid tot de volgende set aan randvoorwaarden die de overheid kan bieden om verticaal evacueren beter mogelijk te maken.

1. Breng per buurt in kaart wat de vluchtmogelijkheden zijn in bestaande woningen en gebouwen. Identificeer vervolgens de noodzaak voor aandacht in beleid voor ruimtelijke ontwikkeling om bestaande bouw te benutten als publieke shelter of buurten prioriteit te geven in preventieve evacuatie.
2. Informeer de bevolking specifiek over zowel preventieve als verticale evacuatie bij overstromingen inclusief wat de situatie betekent naast de algemene risico-informatie.
3. Het kunnen inschatten van de effectiviteit (in termen van slachtoffers, leefbaarheid) van evacuatie gekoppeld aan een vooraf uitgewerkte redeneerlijn voor het wegen van deze informatie door beslissers.
4. Het in beeld hebben van de beschikbaarheid van nuts- en ICT-voorzieningen voor de doorbraak binnen het bedreigd gebied en zo nodig afspraken maken hierover.
5. Het benutten van aanwezige voorraden drinken, voedsel en medicijnen in een gebied en zo nodig afspraken maken met beheerders als supermarkten voor de verspreiding voor de doorbraak.
6. Richtlijnen voor benutting (en behoud) van beschikbare reddings-capaciteit en reddingsoperatie voor bijvoorbeeld locatiekeuzes van coördinatiecentra en kazernes en evacueren van materiaal.
7. Het opzetten van een meldpunt voor hulpbehoevenden waar deze zich gedurende de dreigingsfase kunnen laten registreren als input voor de reddingsoperatie.

Daarnaast is aanbevolen om randvoorwaarden voor verticaal evacueren in combinatie te zien met preventieve evacuatie. Het complete onderzoek is te zien op: http://www.wodc.nl/onderzoeksdatabase/2483-randvoorwaarden-verticale-evacuatie.aspx

Slimmer evacueren bij overstromingen

Het nieuwe waterveiligheidsbeleid in Nederland zet in op reductie van slachtofferrisico's door een combinatie van preventie, ruimtelijke planning en evacuatie. Bij de bepaling van deze slachtofferrisico's zijn de omstandigheden en locatie sterk van invloed op de overlijdenskans (bijvoorbeeld of men schuilt in de eigen woning of onderweg wordt getroffen). Om deze invloed mee te nemen is een nieuwe methode ontwikkeld waarin het aantal slachtoffers wordt bepaald door onderscheid te maken in de klassen: preventieve evacuees, onderweg getroffen, in schuilplaatsen en thuisblijvers (wel en niet voorbereid). De methode levert bouwstenen om slimmere evacuatiestrategieën te ontwikkelen gegeven de ruimtelijke kenmerken van een gebied. Ook kan de methode worden gebruikt om op de lange termijn de inrichting vanuit de invalshoek van evacuatie te beïnvloeden. Hiermee draagt het bij aan de minimalisatie van het aantal slachtoffers tijdens een overstroming, beperking van de maatschappelijke ontwrichting en risicobeheersing.

Gerbert Pleijter en Bas Kolen
HKV
Bas Jonkman
TU Delft
Arno Bouwman
PBL

In het nieuwe waterveiligheidsbeleid staat het overstromingsrisico centraal. Dit betekent dat ruimtelijke inrichting, planning en rampenbeheersing kunnen worden ingezet als instrument om het aantal slachtoffers, als gevolg van een overstroming, te verminderen en het overstromingsrisico te reduceren (zie ook de PBL studie "Kleine kansen – grote gevolgen" Magazine nationale veiligheid en crisisbeheersing 2014 – nr. 4). In de huidige standaardmethode van Jonkman, zoals gebruikt in het Deltaprogramma, is voor de

bepaling van het aantal slachtoffers alleen een totaalschatting bepaald. In opdracht van PBL ontwikkelde HKV in samenwerking met de TU Delft een verbeterde methode van slachtofferbepaling. Hierbij is onderscheid gemaakt in de toestand en locatie, waardoor de invloed van maatregelen in de ruimtelijke ordening en crisisbeheersing expliciet kunnen worden meegenomen.

In deze verbeterde methode is de getroffen bevolking verdeeld over vijf verschillende categorieën die elk een mogelijke toestand van slachtoffers beschrijft.

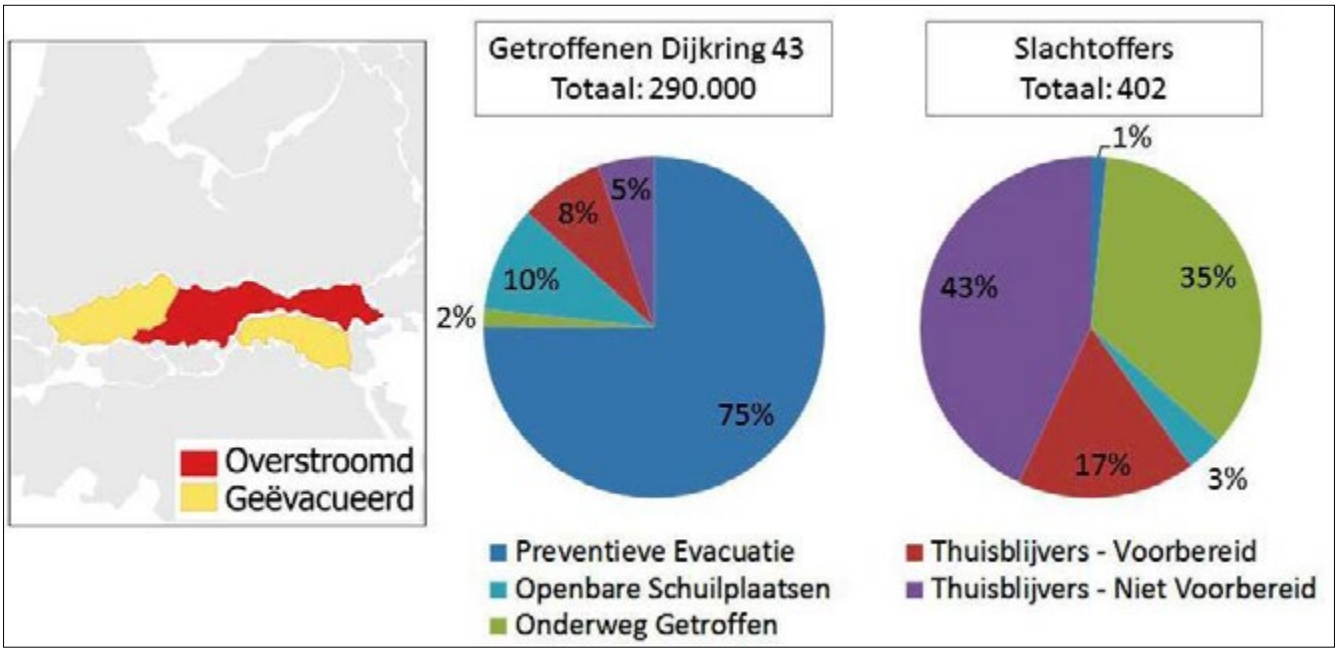
1. Slachtoffers tijdens preventief evacueren, bijvoorbeeld verkeersongevallen.
2. Slachtoffers die tijdens preventieve evacuatie worden overvallen door de overstroming, bijvoorbeeld verdrinking, onderkoeling.
3. Slachtoffers in openbare schuilplaatsen.
4. Slachtoffers onder thuisblijvers die zijn voorbereid, bijvoorbeeld verdrinking.
5. Idem als bij groep 4 maar dan onvoorbereid.

Overstromingen wereldwijd laten zien dat de kwetsbaarheid van deze groepen sterk verschilt. Voor elke categorie is op basis van historische gegevens een slachtofferfunctie afgeleid voor de Nederlandse situatie. Slachtoffers tijdens preventieve evacuatie hebben een zeer kleine overlijdenskans. Personen in openbare schuilplaatsen hebben een overlijdenskans van een orde groter. De overlijdenskans van thuisblijvers is gebaseerd op de standaardmethode van Jonkman welke afhankelijk is van de waterdiepte, stroom- en stijgsnelheid. Hierbij wordt onderscheid gemaakt in een groep die zich wel voorbereid en een groep die dat niet doet, deze zijn dus kwetsbaarder. Mensen die onderweg zijn, hebben een grotere kans te overlijden aan verdrinking en onderkoeling dan de thuisblijvers. De mortaliteit is minimaal 5x hoger in vergelijking met de thuisblijvers en wordt dus ook bepaald op basis van de optredende waterdiepte.

De methode is toegepast binnen dijkring 43 – Culemborger en Tielerwaarden. Hierbij is er rekening mee gehouden dat ook de omliggende dijkringen (41 en 16) evacueren maar uiteindelijk niet overstromen (zie Figuur). In totaal zijn in de drie dijkringen 750.000 mensen getroffen door evacuatie. In het voorbeeld kan 75% van de mensen in dijkring 43 op tijd preventief evacueren, wordt 5% onderweg getroffen, is 10% in een openbare schuilplaats en 10% thuis gebleven. Afhankelijk van de gebiedskarakteristieken (landelijk of stedelijk) brengt een deel van de mensen die onderweg getroffen wordt zichzelf nog in veiligheid. De meeste slachtoffers vallen onder de groepen “niet voorbereide thuisblijvers” en personen die “onderweg getroffen” worden.

De nieuwe methode biedt inzicht in welke categorie slachtoffers vallen. Wanneer het onzeker is of iedereen het gebied tijdig kan verlaten, kan beter (gedeeltelijk) worden ingezet op verticale evacuatie of evacuatie naar openbare schuilplaatsen gezien het grote aantal slachtoffers die onderweg kunnen vallen. Daarnaast kan het risicobewustzijn worden verbeterd om slachtoffers in de groep onvoorbereide thuisblijvers te verminderen.

Met de methode kunnen slimme- en flexibele evacuatiestrategieën worden gerealiseerd die rekening houden met de lokale ruimtelijke inrichting en de beschikbare tijd voor evacuatie (zie ook: Flexibele evacuatiestrategie, Magazine nationale veiligheid en crisisbeheersing 2015 – nr. 1). Op de langere termijn biedt de methode de mogelijkheid bij gebiedsontwikkeling beter rekening te houden met overstromingsrisico’s en evacuatieplanning door bijvoorbeeld extra vluchtplekken of betere vluchtwegen en vluchtplannen te creëren.



Seminar crisisbeheersing zorgsector

"Terroristen dromen van een grote aanslag met een vuile bom. Ziekenhuizen zijn daarvoor belangrijke leveranciers." Rob de Wijk maakt de link tussen terrorisme en de zorgsector in één klap duidelijk tijdens het seminar "Crisisbeheersing zorgsector – Lessen uit recente crisissituaties" op 25 juni in Zeist. In combinatie met de waarschuwing van de AIVD voor spionage in academische ziekenhuizen is duidelijk dat de zorgsector een rol heeft in de crisisbeheersing in Nederland.

Martin Bobeldijk
Turnaround Communicatie (www.turnaroundcommunicatie.nl)

"Wie van u is terrorist?" Rob de Wijk, directeur van het Den Haag Centrum voor Strategische Studies, vindt het opmerkelijk dat veel bekende terroristen een medische achtergrond hebben. Komt het doordat artsen veel met dood en verderf te maken hebben en de stap daardoor kleiner is? Of komt het doordat artsen idealistische mensen zijn, zoals uit de zaal wordt geopperd? Een duidelijk antwoord is er niet. Wel blijkt uit onderzoek dat terrorisme altijd te maken heeft met het bereiken van politieke doelen door middel van geweld. Vanuit dit perspectief gezien is de aanslag op de satirische krant Charlie Hebdo geen bedreiging voor de nationale veiligheid. Het gaat om een enkele aanslag, hoe erg ook. Terrorisme wordt een bedreiging als er een maatschappelijke beweging op gang komt die tot sociale ontwrichting leidt en de politiek destabiliseert. Om dat voor elkaar te krijgen zoeken terroristen specifieke doelwitten uit. Zo is Charlie Hebdo een symbool van het vrije woord. Het World Trade Centre en het Pentagon staan symbool voor het financiële en machtshart van de Verenigde Staten. De wereldkampioenschappen voetbal, kerken en Joodse instellingen zijn andere symbolische voorbeelden. 40 procent van de aanslagen is hierop gericht.

LEVENSGEVAARLIJKE CONSEQUENTIES

Alle andere aanslagen zijn gericht op soft targets om zoveel mogelijk slachtoffers te creëren. De bekendste succesvolle aanslagen zijn die op het openbaar vervoer, zoals in Madrid en Tokio. Volgens De Wijk dromen terroristen ervan grote aanslagen te plegen en proberen ze daarvoor vuile bommen te bemachtigen. Ziekenhuizen moeten hierop alert zijn, want zij zijn belangrijke leveranciers. Zo kan het bijvoorbeeld gaan om bommen die omwikkeld worden met radioactief ziekenhuisafval. "De klap zelf is al vervelend, maar de contaminatie daarna is nog veel vervelender. De opslag, vervoer en destructie van ziekenhuisafval moet daarom goed geregeld zijn." Ook roept De Wijk op alert te zijn op mensen die in behandeling zijn in de geestelijke gezondheidszorg. Veel extremisten zijn beschadigde mensen. Dat is heel opmerkelijk. Uit onderzoek blijkt dat 60 procent psychosociale problemen heeft en 14 procent is in ernstige mate

© Ab Scheel

© Floris Oudshoorn

ontregeld. Verder blijkt dat de gemiddelde leeftijd van extremisten op 27,3 jaar ligt, dat ze met name een Algerijnse, Marokkaanse of Pakistaanse achtergrond hebben en in het criminele circuit verkeren. Volgens De Wijk is de oplossingsrichting voor radicalisering en extremisme het winnen van de "hearts and minds". "Polarisatie is het domste wat je kunt doen. Als je maar hard en vaak genoeg roept dat de Koran en de mensen niet deugen, dan krijg je vanzelf een selffulfilling prophecy. Terughoudendheid is belangrijk en daar zit nou juist het probleem. Mensen worden boos en politici gebruiken dat voor hun eigen positie. Dat heeft levensgevaarlijke consequenties." Voor ziekenhuizen en zorgverleners is het daarom belangrijk rekening te houden met situaties waarin het ernstig misgaat en er een grote toestroom aan slachtoffers op gang komt die zijn weerga niet kent. En waarbij sprake is van een chemische, bacteriologische, radiologische of nucleaire besmetting van slachtoffers en gebieden.

NEDERLAND AANTREKKELIJK DOELWIT

De AIVD merkt op dat Nederland niet alleen te maken heeft met terroristen, maar ook met spionnen. "In Nederland wordt veel gespioneerd. Ook in academische Ziekenhuizen en universiteiten. Ons land staat namelijk bekend om zijn openheid. Wij delen onze kennis, beantwoorden alle vragen van iedereen en zijn blij met iedere buitenlandse student. Buitenlandse inlichtingendiensten maken daar dankbaar gebruik van. Zij sturen studenten en stagiairs naar de Nederlandse kennis en technologie toe, om het vervolgens mee naar huis te nemen." In tegenstelling tot de AIVD hebben buitenlandse inlichtingendiensten meestal tot taak geheimen van

andere overheden te stelen en de economische welvaart en handel in hun land te bevorderen. Nederland is voor hen aantrekkelijk, omdat wij veel internationale organisaties binnen onze grenzen hebben, een hoogwaardige en innovatieve industrie hebben, een kenniseconomie hebben, grote datanetwerken en –bestanden hebben en lid zijn van de EU, NAVO en VN. Ze zijn onder andere uit op persoonsgegevens, databestanden en (nucleaire) technologieën èn op kennis van beveiligingsmaatregelen, ICT-voorzieningen, vitale sectoren en onderzoeks- en kennisinstellingen.

© Floris Oudshoorn

DIGITALE SPIONAGE

„Die Chinese student. Is dat echt een student of doet hij hele andere dingen? Of speelt uw eigen medewerker informatie door in ruil voor geld, seks of andere zaken? Inlichtingendiensten zetten vaak dit soort "human intelligence" in. Wees daar op bedacht. Als AIVD kunnen we niet alles. Wij lopen niet de hele dag in universiteiten en ziekenhuizen rond. U kunt zelf het beste de intenties van iemand inschatten. Wees ook bedacht op contacten in het buitenland, bijvoorbeeld als u naar een internationaal congres gaat. Het kan maar zo dat er contact met uw wordt gelegd met bijbedoelingen. Bel ons als er iets niet klopt." Een nog grotere dreiging is volgens de AIVD digitale spionage. Daarbij wordt vaak gebruikgemaakt van "social engineering". "Bent u daartegen bestand? Ik ben van mening dat mensen op gevoelige posities in organisaties verplicht terughoudend moeten zijn met social media, om dit te bemoeilijken. En zijn uw systemen bestand tegen spionage? Waarschijnlijk weet u dat niet. Maar weet u wel wat er bij u te halen valt aan kennis, beleid, technologie, "intellectual property", data en dergelijke? In Nederland hebben organisaties een laag bewustzijn als het gaat om veiligheid en spionage. Daarom adviseer ik om hier goed naar te kijken. Beoordeel wat voor u cruciaal is, laat uw medewerkers dat weten en neem daarop uw beschermingsmaatregelen."

VIRUSUITBRAAK

Heel andersoortige beschermingsmaatregelen worden genomen in het Calamiteiten Hospitaal te Utrecht, vertelt internist-infectioloog Pauline Ellerbroek. Hier worden patiënten opgevangen op biosafetylevel 3 en 4. Het gaat dan met name om virussen met een groot ziekmakend vermogen die in staat zijn mensen ernstig ziek te maken, waarvoor vaak geen behandelingsmethode beschikbaar is, die via de lucht worden overgedragen en die een hoge mortaliteit kennen. Voorbeelden zijn sars, pokken en virale hemorragische koorts zoals ebola. Het Calamiteiten Hospitaal heeft vier isolatieboxen met intensive care-mogelijkheden en een opvangmogelijkheid van dertig patiënten op medium en low care. In verband met de ebola-uitbraak in 2014 is besloten dat militairen en buitenlandse gezondheidsmedewerkers in het Calamiteiten Hospitaal worden opgevangen. Gerepatrieerde Nederlanders gaan naar andere ziekenhuizen. In december 2014 heeft het Utrechtse ziekenhuis een Nigeriaanse militair opgevangen. In de voorbereiding hierop is een multidisciplinaire werkgroep van medici, beleids- en personeelsmedewerkers, logistiek en bewaking aan de slag gegaan. Zij hebben alle procedures tegen het licht gehouden, scenario's getoetst en de crisisorganisatie uitgewerkt. Ten opzichte van het reguliere Ziekenhuis Rampenopvangplan (ZiROP) zijn er diverse wijzigingen doorgevoerd in de voorbereidings-, meldings-, besluitvormings- en alarmeringsfase. Ook zijn er plannen en "flow charts" gemaakt voor onverwachte patiënten die de hoofdingang van het ziekenhuis binnenlopen. En de locatie zelf is op onderdelen aangepast. Zo zijn de wasbakken afgesloten om verontreinigde afvalwaterlozingen te voorkomen en zijn er sloten op de deur geplaatst om te voorkomen dat besmette patiënten de deur uitlopen.

© Ab Scheel

BESCHERMINGSMAATREGELEN

Het personeel is volgens Ellerbroek uitgebreid getraind op het nemen van persoonlijke beschermingsmaatregelen. "Instructiefilms en -kaarten leggen uit hoe je jezelf moet aan- en uitkleden. Ook hebben we een buddysysteem geïntroduceerd. Dat was compleet nieuw en moest daarom goed getraind worden. De buddy leidt de verpleegkundige door het hele aan- en uitkleedproces. Ook leest hij via een headset alle instructies voor die de verpleegkundige ondertussen uitvoert bij de patiënt in de isolatiebox. Door de beschermende kleding moet je na 45 minuten afgelost worden. Dat dwingt je om van te voren goed na te denken over wat je gaat doen bij de patiënt. Met hulp van de buddy die buiten de box staat en toekijkt via een raam, kun je efficiënt en effectief handelen." Ook is er geoefend met ambulancediensten. Een leerzame les volgens Ellerbroek, want vlak voor de komst van de Nigeriaan bleek dat protocollen niet op elkaar aansloten. De man heeft uiteindelijk 12 dagen in het Calamiteiten Hospitaal gelegen.

BIJZONDERE UITVAARTEN

Voor het geval er dodelijke slachtoffers zijn te betreuren als gevolg van een aanslag, staat het "team bijzondere uitvaarten" van Monuta klaar. Hans Bleijerveld is directeur van dit team. "Wij hebben met vrijwel alle veiligheidsregio's een convenant en we zijn wereldwijd inzetbaar. Wij worden ingezet bij rampen en calamiteiten in binnen- en buitenland waar Nederlanders bij betrokken zijn.

Hiervoor zijn we speciaal getraind, onder andere door Defensie. De meeste recente ceremonie en uitvaart die we hebben verzorgd, was die van de slachtoffers van de crash met de MH17 in Oekraïne." Volgens Bleijerveld is iedere ramp en calamiteit anders. Daarom heeft hij geen draaiboeken klaarliggen. "Dat zet je vast in bepaalde gedachten en dat wil ik niet. Iedere keer wil ik aanvoelen wat de situatie is en wat daarbij past. Wij leveren maatwerk. En dat zit 'm vaak in de kleinste details." Binnen 24 uur is het aankomstceremonieel en het staatsievervoer uitgedacht en geregeld, in samenwerking met een grote groep deskundigen van Defensie en andere (overheids) organisaties. Vervolgens zoekt Bleijerveld 74 collega's om de nabestaanden te begeleiden, omdat deze professionals kunnen omgaan met rouwende mensen en hun emoties. Ook worden 60 zwarte auto's geregeld. Deze worden speciaal gerangschikt op merk, zodat het één stoet lijkt van dezelfde zwarte auto's. De chauffeurs worden vlak van te voren nog getraind om op vijf meter afstand van elkaar te rijden. "Op die manier laten we één stoet zien, als symbool van de eenheid en het verdriet dat in Nederland wordt ervaren."

© *Floris Oudshoorn*

KRITIEKE MOMENTEN EN BESLUITEN

Marco Zannoni, directeur van COT Instituut voor Veiligheids- en Crisismanagement, deelt de visie van Bleijerveld dat draaiboeken, protocollen en processen het gevaar in zich hebben je te vangen in een bepaalde structuur. "Ik adviseer je zo flexibel mogelijk te reageren. Het gaat er om wat de situatie op dat moment van je vraagt. Maar hoe weet je dat? De ene crisis begint klein en wordt groot. De andere crisis pak je groot aan, terwijl het klein blijft. Hoe kun je daar beter op inspelen?" Het COT heeft daarvoor een model ontwikkeld met 16 impactgebieden, zoals zorg(continuïteit), externe communicatie, ketensamenwerking, onderzoek, juridische aspecten en schade. "Aan de hand van dit model kun je een diagnose maken en inschatten op welke gebieden je crisis impact heeft. Vervolgens kun je daarop acteren." Daaraan voorafgaand adviseert Zannoni in de crisisvoorbereiding vooral te focussen op kritieke besluiten en kritieke momenten. Die maken het verschil. Kritieke besluiten zijn bijvoorbeeld evacuaties, het voor het eerst naar buiten gaan met informatie die nog niemand heeft of iemand op non-actief zetten. Kritieke momenten zijn bijvoorbeeld een eerste persconferentie, presentatie van onderzoeksresultaten of een rechtszaak. "Door de combinatie van diagnose stellen en focussen op kritieke momenten en besluiten, treed je een crisis slim tegemoet."

Voor meer informatie zie: www.svdc.nl

Cyberoefening **ISIDOOR**

De NCTV organiseerde samen met dertig publieke en private partners van 22 tot en met 25 juni de operationele cyberoefening ISIDOOR. Er werden cyberincidenten gesimuleerd waarbij er sprake was van datalekken en kwetsbaarheden in systemen. De overheid moest in samenwerking met publieke en private partijen beslissingen nemen over de operationele respons op het betreffende incident.
Doel was om de gezamenlijke aanpak, samenwerking en coördinatie te testen bij een cybercrisis. Aan de oefening deden 200 spelers mee. Naast alle operationele diensten op het gebied van cyber security hebben ook diverse ministeries, uitvoeringsorganisaties en partners uit onder meer de telecom- energie- en financiële sector mee geoefend. De oefening was opgebouwd uit een decentraal deel waarbij deelnemers in hun eigen werkomgeving oefenden en een centrale oefendag waarbij centraal gezamenlijk een afsluitende oefening werd uitgevoerd. In Nederland werken veel private en publieke partijen samen in de respons op cybercrises en –incidenten. Het Nationaal Cyber Security Centrum coördineert deze samenwerking. ISIDOOR had tot doel om de afspraken op dit terrein te testen en zo de samenwerking verder te verbeteren. Oefeningen, zoals ISIDOOR, zijn van groot belang om deze ontwikkeling en meer specifiek de Nederlandse capaciteit voor respons op cyberincidenten en crises vorm te geven. Publiek-private samenwerking is daarbij van groot belang; het overgrote deel van de ICT-infrastructuur in Nederland is in handen van private partijen en het beschermen van vitale belangen in het digitale domein is een gezamenlijke verantwoordelijkheid.

VERSTERKING DIGITALE VEILIGHEID VAN NEDERLAND

Cyberincidenten die zich de afgelopen paar jaar hebben voorgedaan laten zien hoe kwetsbaar de Nederlandse samenleving is als gevolg van de steeds verder toenemende digitalisering. Het verhogen van de digitale weerbaarheid van Nederland is daardoor van groot belang. Met de vaststelling van de tweede Nationale Cyber Security Strategie is daarom besloten tot het uitwerken van een integrale aanpak van cyberdreigingen. De oefening is uitwerking van een van de acties binnen deze aanpak.
(bron: *Nieuwsbericht NCTV*)

Sociale media en crises:
tips voor overheden en burgers

Sociale media zijn niet meer weg te denken uit de samenleving. In toenemende mate worden ze ook gebruikt tijdens crises, maar hoe kunnen sociale media nu adequaat (dat wil zeggen effectief en met beperkte risico's) gebruikt worden bij de bestrijding van rampen en crises en waarvoor precies? Dit was het onderwerp van het tweejarig Europese FP-7 onderzoeksproject COSMIC: the COntribution of Social Media In Crisismanagement. Het project heeft geresulteerd in een concrete en praktische set met tips voor overheden over hoe sociale media adequaat te gebruiken voor, tijdens en na crisissituaties. Daarnaast is een vergelijkbare set met tips opgesteld voor burgers over hoe zij met name tijdens crisissituaties sociale media kunnen gebruiken om zichzelf en anderen, inclusief overheden en andere organisaties, te helpen.

Ira Helsloot
Hoogleraar Besturen van Veiligheid Radboud Universiteit / Crisislab
Gaby van Melick
Crisislab
Nico van Os
Veiligheidsregio Zuid-Holland Zuid

SOCIALE MEDIA IN CRISES

Het is een gegeven dat de informatiebehoefte zeer hoog is tijdens crises: overheden en (hulpverlenings)organisaties, maar ook burgers hebben informatie nodig om adequaat op een crisis te kunnen reageren. Dit terwijl bij crises informatie veelal schaars is. Via sociale media is in toenemende mate snel, relevante informatie beschikbaar, die bovendien eenvoudig en snel (verder) verspreid kan worden in de samenleving. Dat nagenoeg iedereen kan deelnemen is de kracht van sociale media: het biedt ook niet-traditionele partijen – zoals burgers – een manier om eenvoudig informatie te verspreiden en/of zich en anderen te organiseren om hulp te bieden. Tegelijkertijd brengt juist het laagdrempelige en grootschalige gebruik van sociale media risico's en problemen met zich mee: bijvoorbeeld de verspreiding van onbetrouwbare of onverifieerbare informatie en inbreuken op de privacy.

FUNDAMENT VAN DE TIPS

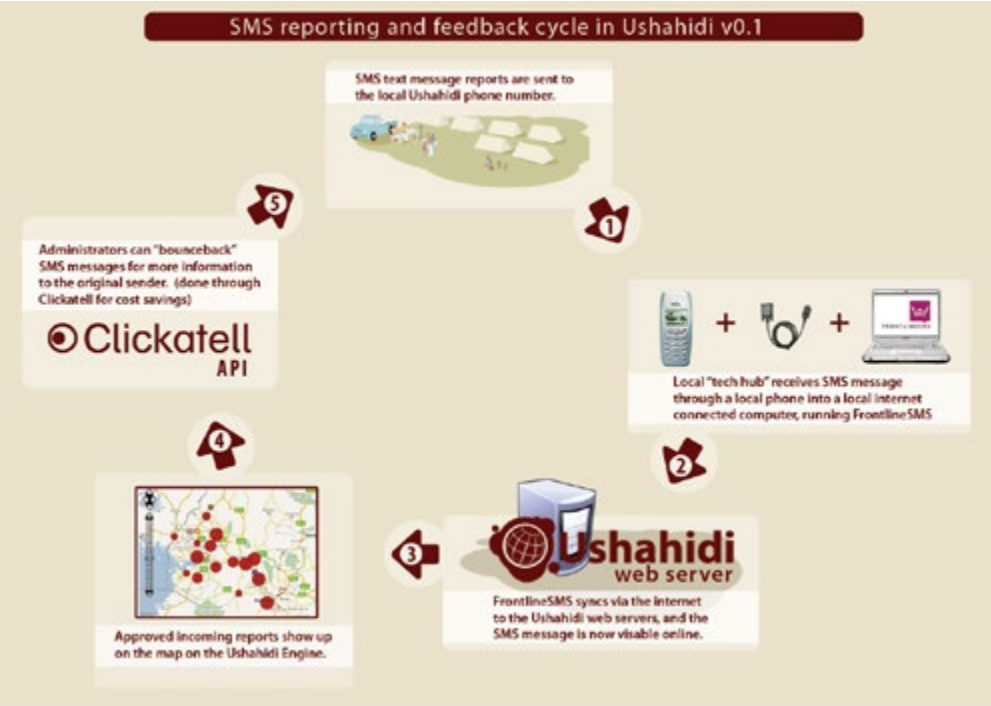
Een belangrijk inzicht in COSMIC is dat burgers zeer actief en zelfs (zelf)redzaam zijn tijdens crises. Zij ondernemen succesvol verschillende soorten actie om zichzelf, naasten, maar ook vreemden en zelfs hulpverleningsorganisaties te helpen.

Met name direct na een crisis, wanneer hulpdiensten vaak nog niet aanwezig zijn, kunnen burgers hiermee een belangrijke aanvulling op en ondersteuning van de hulp geboden door hulpverleningsorganisaties vormen. Deze hebben namelijk tijdens crises, gezien de omvang en diversiteit van de uit te voeren taken en de tijdsdruk, zelden voldoende capaciteit om op alle behoeften in te spelen. Om zich op de meest prangende gevallen, waar hulp onontbeerlijk is, te kunnen focussen, is het noodzakelijk dat zoveel mogelijk burgers gefaciliteerd worden zichzelf en eventueel hun naasten in veiligheid te kunnen

Occupy Sandy: voorbeeld van burgerinitiatief na orkaan Sandy waarin burgers eigen hulpvoorziening, schoonmaak- en wederopbouwactiviteiten organiseerden.

brengen. Informatie over de situatie is hiertoe een kernvoorwaarde: hoe meer inzicht in de situatie hoe beter burgers kunnen reageren. Het is dus belangrijk dat de informatie die overheden en hulpverleningsorganisaties ontvangen ook naar burgers verspreid wordt. Sociale media zijn hierbij een effectief middel.

Bovendien zoeken hulpdiensten juist meer inzicht in de situatie om hun hulpverlening effectiever vorm te geven. Burgers zijn daarvoor een belangrijke bron. Niet alleen als ooggetuigen ter plaatse maar ook als zij in een wiki-vorm informatie bundelen. Natuurlijk bestaan er risico's, zoals onbetrouwbare informatie, maar het onderzoek dat in COSMIC is bijeengebracht laat zien dat de voordelen van vertrouwen op burgerinformatie veel groter zijn dan de nadelen. Het platform *Ushahidi*, gebruikt na onder andere de aardbeving in Haïti,



Ushahidi toont burgers hoe zij (zelfs van een afstand) kunnen bijdragen in de hulpverlening en het toont overheden en hulpverleningsorganisaties een verantwoorde wijze van inzet van burgers bij informatieverzameling en verificatie.

is een voorbeeld van een initiatief waar burgers zelf informatie verzamelen en verifiëren en dat organisaties als het Rode Kruis en InStedd helpt bij de coördinatie van de hulpverlening.

Ter vergroting van de efficiëntie van crisishulpverlening is het daarmee bevorderlijk dat overheden zich aanpassen aan burgerinitiatieven via sociale media, zoals Ushahidi, die in de maatschappij ontplooid (en dus gedragen) worden. Zeker omdat de overheid bijna onvermijdelijk achterloopt op de samenleving bij de ontwikkeling en toepassing van sociale media.

Deze inzichten hebben geresulteerd in een drietal principes die aan de basis liggen van de tips voor burgers en overheden.

- *Erkennen* dat de maatschappij vertrouwd kan worden.
- *Stimuleren* van de capaciteit van de maatschappij om zelf verantwoordelijkheid te dragen voor haar welzijn.
- *Ontwikkelen* van de capaciteit van overheden zich aan te passen aan het gebruik van sociale media door de maatschappij.

TIPS

Op basis van bovenstaande inzichten zijn tips opgesteld die overheden en burgers helpen sociale media op een effectieve en verantwoorde manier te gebruiken bij crises om informatie te verspreiden en/of te verzamelen. Prominente onderwerpen zijn bijvoorbeeld: hoe heeft informatie impact, hoe kan informatie geverifieerd of verifieerbaar aangeboden worden en hoe kan privacy gewaarborgd worden.
Om te komen tot een handzame gids met tips zijn de tips voor overheden georganiseerd per fase waarin zij actief zijn: de voorbereiding op crises, de crisis en na afloop van een crisis: de herstelfase. De tips voor burgers zijn georganiseerd naar de activiteiten die zij met name tijdens crises ondernemen, omdat zij bij uitstek in deze fase actief zijn. Zo zoeken of verstrekken burgers hulp, zoeken of verstrekken zij informatie of mobiliseren zij anderen om hulp te verstrekken. Hulp is hierbij een breed begrip: van EHBO tot onderdak en andere hulpmiddelen, tot assistentie bij het verzamelen en verwerken van data: zoals het compileren van slachtofferlijsten, tot het opzetten van fondsenwerving. De tips zijn voorzien van concrete stappen en van voorbeelden.

De meest recente versie van de guidelines is te vinden op www.crisislab.nl en www.cosmic-project.eu. De tips moeten gezien worden als een eerste stap in het bieden van handvaten voor het optimaal benutten van sociale media in de aanpak van crises en rampen. Als zodanig is verdere ontwikkeling en verfijning noodzakelijk, bijvoorbeeld door diezelfde veerkrachtige civil society en overheden die geadresseerd worden. Commentaar is dan ook van harte welkom, bijvoorbeeld via de auteurs.

Krachten risico-regelreflex beschreven in 27 voorbeelden

De risico-regelreflex is een term die sinds zijn introductie in 2010 steeds meer gebruikt en herkend wordt door onder andere bestuurders, volksvertegenwoordigers en ambtenaren. De risico-regelreflex is de valkuil om zonder goed na te denken na incidenten of media-aandacht voor risico's meteen te besluiten tot extra veiligheidsmaatregelen. Adequaat omgaan met de risico-regelreflex is een van de voorwaarden van goed bestuur. Het herkennen van de risico-regelreflex is een belangrijke eerste stap in het vermijden ervan. Maar hoe herken je de risico-regelreflex?

- **Astrid Scholtens**
  Onderzoeker Crisislab
- **Ira Helsloot**
  Hoogleraar Besturen van Veiligheid Radboud Universiteit Nijmegen/ Crisislab

Om de risico-regelreflex te kunnen herkennen is inzicht wenselijk in de krachten die de risico-regelreflex in het besluitvormingsproces versterken of verzwakken. Dit worden "aanjagende" respectievelijk "dempende krachten" genoemd. Crisislab heeft met subsidie van het ministerie van BZK in 27 casussen (waarin - na het openbaar worden van een risico - veiligheidsbeleid is ontwikkeld) het optreden van de risico-regelreflex onderzocht en daarbij een aantal onderliggende aanjagende en remmende krachten gevonden.

Een voorbeeld van een aanjagende kracht is: "Veiligheid is dé kerntaak van de overheid". Bij sommigen heerst een diepe overtuiging dat het voorkomen van alle ongevallen dé kerntaak van de overheid is, dat wil zeggen dat de overheid de eindverantwoordelijkheid heeft om zo veel mogelijk risico's te voorkomen. Incidenten zijn in die opvatting dan ook een bewijs van het falen van de overheid, zodat maatregelen genomen moeten worden om herhaling te voorkomen. Een kenmerkende uitspraak die op deze aanjagende kracht wijst, is: "*het is in de eerste plaats de verantwoordelijkheid van de overheid om de veiligheid van haar burgers te garanderen*". In de tabelworden de aanjagende en dempende krachten die door ons zijn geïdentificeerd kort samengevat.

Deze aanjagende kracht was bijvoorbeeld zichtbaar in het teenslipperincident in Maastricht. De gemeente heeft het oud papier ophalen uitbesteed aan een privaat bedrijf dat studenten als vrijwilligers inzet en daarvoor een vergoeding aan hun vereniging geeft. In 2013 raken twee studentes gewond omdat ze met teenslippers aan het oud papier in de kraakwagen willen aanstampen. Een kraakwagen wint altijd, zullen we maar zeggen. Direct na het ongeval legt de gemeente Maastricht het ophalen van het oud papier door alle vrijwilligers stil en zet eigen medewerkers in. De Arbeidsinspectie concludeert na onderzoek dat het ongeval onder andere veroorzaakt is door ondeugdelijke instructie door de private oud papier ophaler en het niet dragen van veiligheidskleding.

Aanjagende krachten	Dempende krachten
De overtuiging dat burgers risico's niet accepteren	Bestuurlijke moed om op basis van feiten te beslissen
Specialistisch advies	Burgers zijn risicorealisten
Oneindige professionalisering van de uitvoering	Vertrouwen in *begrensde* professionaliteit van de uitvoering
Bestuurlijke en politieke dadendrang	Het laten verrichten van een risicovergelijking
Angst voor aansprakelijkheid	Het in beeld brengen van kosten en baten van veiligheidsmaatregelen
Veiligheid is dé kerntaak van de overheid	Expliciet beroep doen op andere waarden dan veiligheid
Veiligheid boven alles	Verantwoordelijkheid van andere partijen expliciet benoemen
Veiligheid als camouflage	Erkenning van het noodlot
Bestuurlijke fragmentatie	Empathie zonder meer
De overtuiging dat ongevallen aantonen dat het systeem gefaald heeft	

De gemeente besluit zonder andere scenario's te overwegen om in lijn met de bevindingen van de Arbeidsinspectie alle vrijwilligers uit te rusten met veiligheidskleding en op te leiden op kosten van de gemeente, want een dergelijk ongeval mag volgens de gemeente niet meer plaatsvinden. Een individuele fout (het dragen van slippers in plaats van deugdelijk schoeisel) leidt daarmee zonder nadere analyse meteen tot verhoudingsgewijs kostbare maatregelen, zodat in deze casus volgens de definitie sprake is van de risico-regelreflex.

Het idee dat veiligheid dé kerntaak van de overheid is, is duidelijk zichtbaar in deze casus. De gemeente voelde zich immers als vanzelfsprekend verantwoordelijk om maatregelen te nemen. De gemeente had het ophalen van oud papier echter al jaren eerder uitbesteed aan een particulier bedrijf, zodat ook dit bedrijf betrokken had kunnen (of zelfs moeten) worden bij het eventueel nemen van veiligheidsmaatregelen. Een ander voorbeeld van een aanjagende kracht in dit voorbeeld was het idee dat er een wereld bestaat waarin geen ongevallen (zouden moeten) plaatsvinden. Elk incident dat gebeurt, is daarmee een bewijs dat er fouten gemaakt zijn die in de toekomst voorkomen moeten worden. Er moeten dus maatregelen genomen worden, ongeacht de kosten.

De reden dat bij bestuurlijke besluitvorming de risico-regelreflex voorkomen moet worden, is ook meteen zichtbaar in deze casus: de risico-regelreflex kan leiden tot het nemen van disproportionele maatregelen. Dit zijn maatregelen waarvan de baten bij nadere beschouwing duidelijk niet opwegen tegen de kosten en de bijwerkingen, of waarbij de overheid een grotere rol krijgt dan nodig of realiseerbaar is.

In het voorbeeld van het papier ophalen in de gemeente Maastricht heeft de risico-regelreflex geleid tot een waarschijnlijk disproportionele maatregel. Het ging immers om een eenmalig incident. De casuïstiek gaf daarmee geen aanleiding dat dergelijke veiligheidseisen ook echt noodzakelijk zijn, zodat het niet voor de hand ligt dat in deze casus de kosten van naar schatting ongeveer € 70.000,= incidenteel en ongeveer € 63.000,= structureel voor het opleiden en uitrusten van vrijwilligers zullen opwegen tegen de baten.

Een klassiek voorbeeld waarin behalve de dempende kracht "bestuurlijke moed" vooral de dempende kracht "risicovergelijking" heeft geleid tot beheersing van de risico-regelreflex is de casus van de al dan niet sluiting van de metro Oostlijn in 2012. Door een specialistische en daarmee veelal eenzijdig adviserende adviseur werd aanbevolen de metro te sluiten omdat deze op dat moment nog niet aan alle sinds 2005 ingevoerde veiligheidseisen voldeed. Wethouder Wiebes besloot dat de metro openbleef en legde dat uit aan de samenleving door het risico met een ander risico te vergelijken. Door sluiting van de metro zou iedereen op een andere manier naar de binnenstad moeten, terwijl van alle vervoersvormen de metro verreweg de veiligste is. Fietsen bijvoorbeeld, zo stelde hij, is duizendmaal gevaarlijker, dus het wegnemen van het kleine gevaar op een metro-ongeval zou velen dwingen tot het nemen van een groter risico om naar bijvoorbeeld hun werk in de binnenstad te gaan.

Risicovergelijking kan dus helpen als dempende kracht, omdat het door vergelijking duidelijk kan worden dat het snel nemen van maatregelen tegen heel kleine risico's evident disproportioneel is, zeker als daardoor een groter risico nog verder wordt vergroot. Een kenmerkende uitspraak die op deze dempende kracht wijst, is *"dit risico is vergelijkbaar met het risico dat ..."*.

De 27 casus geven een gemengd beeld van situaties waarin toegeven aan de risico-regelreflex miljarden heeft gekost maar ook van situaties waarin door adequate beheersing ervan de samenleving veel materiële en immateriële kosten is bespaard.

Het boek *Krachten rond de risico-regelreflex beschreven en geïllustreerd in 27 voorbeelden* is een laatste product van het interdepartementale programma Risico's en verantwoordelijkheden dat in de periode 2010 – 2014 oorzaken van en remedies tegen de risico-regelreflex onderzocht op veel terreinen. Het kan besteld worden bij Boom | Lemma uitgevers.

Herintreding zedendelinquenten

Marieke Liem
Senior Researcher, Universiteit Leiden, Centre for Terrorism and Counterterrorism, Kennisnetwerk Collectief Gedrag

Meer dan ooit staat de herintreding van zedendelinquenten in de schijnwerpers. Zedendelinquenten zorgen voor maatschappelijk onbehagen, zeker wanneer kinderen slachtoffer zijn. Thans keren er in Nederland jaarlijks ongeveer 700 zedendelinquenten terug in de maatschappij. Hoewel de herintreding vaak rustig verloopt, veroorzaken enkele van deze gevallen commotie.

PUBLIEKE PERCEPTIE

De huidige publieke perceptie omtrent de herintreding van zedendelinquenten wordt gevormd door een aantal hardnekkige mythes.

Hierbij staat voorop dat gedacht wordt dat de meeste zedendelinquenten opnieuw de fout in zullen gaan. Dit heersende beeld wordt niet ondersteund door wetenschappelijk onderzoek. Het algemene recidivecijfer ligt rond de 60 procent, waarbij de kans op recidive het grootst is voor diegenen die zijn veroordeeld voor een vermogensdelict, en het laagst is voor zedendelinquenten (29%).[1] Onder tbs-gestelde zedendelinquenten worden nog lagere recidivecijfers gerapporteerd (12%).[2]

Een andere mythe betreft dat de aanwezigheid van een veroordeelde zedendelinquent in een buurt gerelateerd is aan het aantal slachtoffers in die buurt. Ook deze veronderstelling wordt niet ondersteund. In de zeldzame gevallen dat zedendelinquenten recidiveren met een pedoseksueel delict, zijn slachtoffers veelal kinderen van familieleden of kennissen, die niet noodzakelijkerwijs in dezelfde buurt wonen.

Dat publieke perceptie en werkelijkheid zo ver van elkaar af liggen, is wellicht niet verwonderlijk. De massamedia hebben de neiging om seksuele delicten te over-rapporteren, zich te richten op veiligheidsaspecten en het probleem als epidemie weer te geven. Volgens sommigen heeft dit geëscaleerd tot het ontstaan van een "sex crime panic".

Demonstratie in Leiden tegen de komst van Benno L © Novum

AMERIKAANSE PRAKTIJKEN

In de Verenigde Staten heeft de onrust rondom herintreding van zedendelinquenten geleid tot het invoeren van specifieke wetgeving, ook wel bekend als "Megan's laws". Deze wetgeving stelt de overheid in staat om buurtbewoners actief op de hoogte te stellen van de komst van zedendelinquenten, huisvesting te weigeren en intensieve supervisie op te leggen. Deze wetgeving beoogt als afschrikmiddel te werken bij herhaalde delicten en therapietrouw te vergroten. Daarnaast zou dergelijke wetgeving inwoners informatie geven die nodig zou zijn om hun kinderen te beschermen.

Tot nu toe laat onderzoek echter zien dat positieve effecten van Megan's laws uitblijven. Er is geen sprake van lagere recidivecijfers en grotere therapietrouw. Bewoners in buurten waar men wordt ingelicht, ervaren daarnaast een grotere mate van angst dan bewoners in buurten waar men niet wordt ingelicht. Onbedoelde neveneffecten voor zedendelinquenten bestaan uit het verlies van werk, bedreigingen en vandalisme. Tevens zouden stigmatisering en verbanning juist recidive in de hand werken. In uitzonderlijke gevallen zijn zedendelinquenten vermoord als gevolg van het openbaar worden van hun identiteit.[3]

Samengevat laten resultaten zien dat de positieve effecten (met andere woorden: het tegengaan van recidive) uitblijven, terwijl onbedoelde neveneffecten een scala van problemen creëren die mogelijk meer kosten in termen van risico op recidive dan dat ze opleveren.

[1] B.S.J. Wartna e.a., Terugval in recidive. Exploratie van de daling in de recidivecijfers van jeugdigen en ex-gedetineerden bestraft in de periode 2002-2010, Den Haag: WODC Cahier 2014-16.

[2] E. Leuw, M. Brouwers & J. Smit, Recidive na de tbs. Patronen, trends en processen en de inschatting van gevaar. *Onderzoek en beleid*. Den Haag: WODC, Ministerie van Justitie, 1999.

[3] L.L. Sample & A.J. Streveler, 'Latent consequences of community notification laws', in: S. H. Decker, L. F. Alaird, & C. M. Katz (Eds.), *Controversies in criminal justice*, Los Angeles: Roxbury, 2003, 353-362.

DILEMMA'S IN HET OPENBAAR BESTUUR

In Nederland is het tot nu toe niet gekomen tot dergelijke Amerikaanse praktijken. Tot voor kort bleef het onbekend wanneer een zedendelinquent zich vestigde in een gemeente. Sinds 2009 is het mogelijk burgemeesters dertig dagen voorafgaand aan de vrijlating van ernstige gewelds- en/of zedendelinquenten te informeren onder de pilot Bestuurlijke Informatievoorziening Justitiabelen (BIJ).[4] Thans kent de pilot 253 deelnemende Nederlandse gemeenten.

Door de informatievoorziening is de rol van de burgemeester bij herintredingssituaties op de voorgrond komen te staan en schept daarbij een aantal dilemma's. Tot nu toe zijn er geen duidelijke richtlijnen voor de communicatie van de informatie. Openbaarmaking is niet verplicht en in sommige gevallen zelfs verboden. Er bestaat veel onduidelijkheid over de positie van de burgemeester. Burgemeesters kunnen in een tweestrijd belanden. Enerzijds het achterhouden van informatie voor het grotere publiek, anderzijds het openbaar maken van informatie, dat mogelijk kan leiden tot verstoringen van de openbare orde en gevaar voor de veiligheid van de ex-delinquent.

DILEMMA'S EN *BEST PRACTICES*

Op basis van diepte-interviews met 16 burgemeesters van Nederlandse gemeenten met 8.000 tot 150.000 inwoners, hebben we getracht in kaart te brengen hoe men naar deze dilemma's handelt, en wat hierin de huidige "best practices" zijn.

Wellicht het grootste dilemma vormt het wel of niet terugkeren naar de gemeente waar de betrokkene voor aanvang van detentie woonde. Burgemeesters zijn verdeeld over deze uitgangspositie. Zo stelt één van hen: "Als een zedendelinquent terugkeert uit detentie dan wil ik mijn eigen delinquent. Ik wil niet de Benno L. uit de wereld, ik wil ook niet bij Pauw en Witteman, ik wil in alle rust mijn eigen zedendelinquent terug." Anderen zijn minder stellig in het "terugnemen" van de eigen zedendelinquent en geven aan, dat dit niet altijd realiseerbaar is. Daarbij worden de resocialisatiemogelijkheden aangedragen als reden, maar ook (vooral in kleinere gemeenten) de bekendheid in de buurt en een eventuele confrontatie met de gemaakte slachtoffers. Een burgemeester vat dit samen als: "Wat eigenlijk leidend moet zijn, is het risico op maatschappelijke onrust en wanneer dat het kleinste is als deze persoon niet terugkeert, dan niet." In dit verband wordt gesproken van een "landelijk uitruilsysteem". Hulp van andere gemeenten is dan geboden.

Een tweede dilemma bij herintreding vormt het wel of niet informeren van de buurt. Hierbij geven vrijwel alle burgemeesters aan dat iedere casus een eigen afweging met zich meebrengt. Was de betrokkene woonachtig in de gemeente voorafgaand aan detentie? Heeft betrokkene slachtoffers gemaakt in de buurt? Hoe groot is de kans dat de bewoners op andere wijze aan deze informatie komen? Indien men er voor kiest om de buurt op de hoogte te stellen, geldt als "best practice" het organiseren van een buurtbijeenkomst. Naast het informeren van bewoners, dienen buurtbewoners het gevoel te krijgen dat er naar hen geluisterd wordt en de mogelijkheid te krijgen emoties te ventileren.

Bij ieder van deze dilemma's benadrukken de geïnterviewde burgemeesters het belang van maatwerk, zoals één van hen verwoordt: "Je kunt het zien als een gereedschapskist. Elke keer trek je de kist open en kijk je welk instrumentarium in dat geval het meest gepast is." Deze instrumentaria variëren sterk tussen burgemeesters – sommigen zoeken voorafgaand aan herintreding actief contact met de delinquent in de gevangenis, anderen zijn veel terughoudender: "Het enige wat wellicht handig is om een wijkagent langs te sturen om te laten weten dat we op de hoogte zijn." Welk instrument ook gekozen wordt, openheid en vertrouwen binnen de driehoek tijdens een casus wordt als cruciaal benoemd om een "zachte landing" van de ex-gedetineerde te bewerkstelligen.

Naast de nodige dilemma's, kent de status quo ook een aantal hiaten. De belangrijkste vormt de beoogde dertig-dagen termijn waarop de informatie bekend wordt gemaakt aan gemeenten – in de praktijk varieert dit van een paar weken tot een paar dagen. In sommige gemeenten bleken verlofmeldingen pas achteraf, of geheel niet te zijn gemeld. Dit kan problemen geven in het tijdig vinden van huisvesting of in het nemen van maatregelen. Tevens zijn burgemeesters van mening dat er beperkte bestuurlijke maatregelen voorhanden zijn, zeker wanneer de betrokkene terugkeert naar de eigen koopwoning. Juridische stappen, zoals gebiedsverboden, worden als zeer lastig ervaren en vormen de uitzondering in plaats van de regel.

HOE VERDER?

Met in ons achterhoofd het feit dat Amerikaanse praktijken niet de beoogde resultaten laten zien is het belangrijk om de BIJ voort te zetten op basis van het delen van kennis en ervaring. De prioriteit betreft het oplossen van hiaten in de informatievoorziening op zowel nationaal als lokaal niveau. Op nationaal niveau behelst dat het aanscherpen van de BIJ en zorgen voor het tijdige doorgeven van relevante informatie. Op lokaal niveau dient men nadere invulling te geven aan de maatregel. Hierbij staat kennisdeling, bijvoorbeeld via de digitale leeromgeving "Handelingskader BIJ", voorop. Tot nu toe is veel vooruitgang geboekt in het creëren van creatieve, slimme oplossingen om de herintreding van zedendelinquenten zo goed mogelijk te laten verlopen. Het centraal blijven stellen van maatwerk gecombineerd met openheid en vertrouwen binnen de driehoek kunnen tezamen als leidraad fungeren voor verdere voltooiing.

[4] Via een BIJ-melding worden gemandateerde contactpersonen binnen de gemeente geïnformeerd over de terugkerende delinquent. Deze informatie omhelst basale gegevens over de betreffende persoon, het delict, en eventuele voorwaarden die bij het vonnis of de voorwaardelijke vrijheidstelling (VI) zijn opgelegd. De gemeente kan nadere informatie opvragen bij ketenpartners zoals reclassering, politie en OM. Vervolgens kan door de gemandateerde beleidsmedewerker en/of de burgemeester een analyse worden gemaakt over het risico op verstoring van de openbare orde wanneer de delinquent terugkeert in de desbetreffende gemeenten.

"GRENZEN SLECHTEN"

Jaardag NAC - 23 september 2015

Bent u van mening dat het voor een goede samenwerking bij een crisis noodzakelijk is om verder te kijken dan organisatie- en landsgrenzen? Of bent u daar juist nog niet (helemaal) van overtuigd? Dan is de Jaardag van de Nationale Academie voor Crisisbeheersing op 23 september a.s. iets voor u. Er zijn vele grenzen om te overbruggen, bijvoorbeeld virtueel, organisatie, regionaal en nationaal. Op basis van het thema "grenzen slechten" willen we met u ontdekken hoe we over die grenzen heen komen en welke mogelijkheden/kansen er zijn om kennis en kennissen buiten de eigen organisatie op te doen.

De jaardag biedt u een inspirerende bijeenkomst, met gelegenheid tot het opdoen van nieuwe informatie en kennissen. Reserveer nu alvast **woensdag 23 september van 12.00 tot 17.00 uur** in uw agenda.

LOS ALS ORGANISATIEVORM OPGEHEVEN

De Landelijke Operationele Staf (LOS) bestaat per 1 juli 2015 niet meer als organisatievorm. Het Landelijk Operationeel Coördinatie Centrum (LOCC) voert per die datum de taken van de LOS uit, zoals ze altijd al deden in niet opgeschaalde situaties. De taken bestaan uit het leveren van een operationeel advies om bestuurlijke besluiten te kunnen uitvoeren voor nationale rampenbestrijding en crisisbeheersing. Daarbij wordt ook gekeken naar de beschikbaarheid van mensen en middelen.

Het besluit om de LOS op te heffen, is gebaseerd op adviezen uit onderzoek van onder andere de Algemene Rekenkamer van 2014. Op basis daarvan is de NCTV in samenwerking met haar ketenpartners in de crisisbeheersing, momenteel onder meer bezig met een heroriëntatie op taak en rol van een landelijke operationele organisatie voor de bovenregionale en nationale crisisbeheersing.
Landelijke operationele advisering is en blijft een essentieel onderdeel van een adequate crisisbesluitvorming. De structuur waarin die advisering plaatsvindt, moet echter worden aangepast aan andere in gang gezette wijzigingen binnen de nationale crisisbesluitvorming. De eerste voorstellen voor een nieuwe structuur voor operationele advisering en de mogelijkheid en wenselijkheid van landelijke operationele coördinatie en sturing zullen nog dit jaar worden gepresenteerd.

(bron: Nieuwsbericht NCTV, 25 juni 2015)

Colofon

REDACTIEADRES MAGAZINE NATIONALE VEILIGHEID EN CRISISBEHEERSING

Ministerie van Veiligheid en Justitie
Nationaal Coördinator Terrorismebestrijding en Veiligheid,
kamer Z.06.136
Postbus 20301
2500 EH Den Haag
E-mail: magazine@nctv.minvenj.nl
Internet: www.nctv.nl

REDACTIECOMMISSIE

Redactiecommissie: Marcel van Eck, Paul Abels, Chris van Duuren, Chris Hanekamp, Eelco Jehee, Hedzer Komduur, Martine van de Kuit, Jan-Bart van Oppenraaij, Eelco Stofbergen, Maaike van Tuyll, Geert Wismans (samenstelling en eindredactie)

REDACTIERAAD

Prof. dr. Ben Ale (Technische Universiteit Delft)
Prof. dr. ir. Marjolein van Asselt (Wetenschappelijke Raad voor het Regeringsbeleid/Universiteit Maastricht)
Prof. dr. Edwin Bakker (Universiteit Leiden/ Centre for Terrorism & Counterterrorism)
Dr. Arjen Boin (Universiteit Utrecht)
Mr. dr. Ernst Brainich (zelfstandig onderzoeker en juridisch adviseur)
Prof. dr. Adelbert Bronkhorst (TNO Defensie en Veiligheid)
Prof. dr. Jan van Dijk (Universiteit Twente)
Dr. Menno van Duin (Nederlands Instituut Fysieke Veiligheid)
Prof. dr. Michel van Eeten (Technische Universiteit Delft)
Prof. dr. Georg Frerks (Universiteit Utrecht/ Nederlandse Defensie Academie)
Prof. dr. Beatrice de Graaf (Universiteit Utrecht)
Prof. dr. Bob de Graaff (Universiteit Utrecht/ Nederlandse Defensie Academie)
Prof. dr. Ira Helsloot (Radboud Universiteit Nijmegen)
Prof. dr. Erwin Muller (Universiteit Leiden)
Dr. Astrid Scholtens (Crisislab)
Prof. dr. Rob de Wijk (Universiteit Leiden)

AAN DIT NUMMER WERKTEN MEE

Richard Addae, Frank Bekkers, Renée Bergkamp, Rob Bertholee, Martin Bobeldijk, Marc Bökkerink, Johanna Breuning, Mathilda Buijtendijk, Sladjana Cemerikic, Paula Faber, Han Fennema, Georg Frerks, Sabine Gielens, Jasper Groos, Sven Hamelink, Jetske Hebbink, Ira Helsloot, Tanja Jans, Rob Jastrzebski, Abderrahman Kaouass, Nico Kaptein, Monika John-Koch, Marieke Klaver, Mel Kroon, Marieke Liem, Coby van der Linde, Gert-Jan Ludden, Eric Luiijf, René Marchal, Minke Meijnders, Gaby van Melick, Bert van der Oord, Willem Oosterveld, Marieke Oosthoek, Nico van Os, Marc van Oudheusden, Rob Peters, Cees Pisuisse, Frans Paul van der Putten, Genserik Reniers, Jan Rood, Tie Schellekens, Astrid Scholtens, Dick Schoof, Kelsey Shantz, Niels Smit, Gerke Spaling, Stephan de Spiegeleire, Peter Spijkerman, Marcel Spit, Kathrin Stolzenburg, Tim Sweijs, Teun Terpstra, Maureen Turina, Peter Vaessen, June Vasconcellos, Sara Vernooij, René de Vries, Lodewijk van Wendel de Joode, Rob de Wijk, René Willems, Reinder Woldring, Marco Zannoni, Erwin van der Zwan

FOTOGRAFIE

Gasunie, Havenbedrijf Rotterdam, Ministerie van Defensie, Novum, NCTV, Ab Scheel, Dieter Schütz (Pixelio.de), Shutterstock, Martien Versteegh/Donkigotte

CARTOONS

Floris Oudshoorn

ILLUSTRATIES

BBK, Clingendael, Crisislab, DNV-GL, HCSS, HKV Lijn in Water, Onderzoeksraad voor Veiligheid, Respons, TNO, Wandverslag.nl

VORMGEVING & DRUK

Xerox/OBT, Den Haag

ISSN 1875-7561

Voor een gratis abonnement mail: magazine@nctv.minvenj.nl
Het magazine is te downloaden via www.nctv.nl

4 VR?G?N ??N

MEL KROON
CEO TenneT

1. WAAR LIGT VOLGENS U HET GEZAMENLIJK BELANG TUSSEN OVERHEID, BEDRIJFSLEVEN EN WETENSCHAP?

"Elektriciteit is essentieel en de motor van onze samenleving. Aangezien het transport van elektriciteit aan de basis ligt van de energievoorziening is de samenwerking tussen overheid, wetenschap en TenneT per definitie een gemeenschappelijk belang. Om de leveringszekerheid te waarborgen en het net te beschermen tegen storingen door technisch falen, weers- of natuurinvloeden of door moedwillig handelen (security) werken we nauw samen. De overheid is een belangrijke partner als het gaat om uitbreidingen van het net en het aanpassen van het wettelijke kader, bijvoorbeeld in de ontwikkeling van een net op zee. Daarnaast werkt TenneT samen met diverse instituten voor onderzoek naar technologische innovatie. De toename van duurzame energiebronnen, decentrale opwekking en de toenemende participatie van lokale stakeholders vereisen een nieuwe aanpak. Samen met overheid en wetenschap zorgen we voor de ontwikkeling en instandhouding van een robuust en toekomstbestendig elektriciteitsnet.
Ook voor het aspect security hebben we een intensieve werkrelatie met de overheid. Voor de gezamenlijke bestrijding van koperdiefstal heeft TenneT destijds met de voormalige Minister Opstelten het convenant Koperslag getekend. Daarnaast komt de samenwerking ook sterk terug in de Cyber Security Raad waar Ben Voorhorst, onze operationeel directeur, zitting in heeft namens de vitale sectoren."

2. OP WELKE WIJZEN WERKT U SAMEN MET DE ANDERE VITALE ORGANISATIES?

"Vanzelfsprekend zitten in de elektriciteitsketen van opwekking tot consumptie meerdere partners. Samenwerking is hier een voorwaarde voor het dagelijks functioneren van de energievoorziening. Daarnaast werken we intensief samen met de andere vitale organisaties via bijvoorbeeld Netbeheer Nederland maar ook in de commissie vitale infrastructuren (CVI) van VNO NCW. Onlangs hebben alle partijen in de value chain van TenneT op initiatief van Shell en TenneT meegedaan met een project waarbij alle kritische processen op een rij zijn gezet. Hier is beoordeeld of er processen zijn die in een enkel bedrijf afzonderlijk misschien als minder kritisch worden ingeschat, maar in de totale keten wel kritisch zijn. Het erkennen van elkaars afhankelijkheden zorgt voor een betere samenwerking."

3. TENNET OPEREERT IN NEDERLAND EN IN DUITSLAND; ZIJN ER GROTE VERSCHILLEN IN AANPAK EN PRAKTIJK?

"In Nederland zijn wij als enige verantwoordelijk voor het transport van elektriciteit. In Duitsland doen we dat gezamenlijk met drie collega bedrijven/TSO's. Op het gebied van publieke private samenwerking zijn er ook verschillen. In Nederland heeft bijvoorbeeld een manager van TenneT mede namens Prorail, Shell, Gasunie en KPN twee jaar als volwaardig MT-lid van het Nationaal Cybersecurity Centrum gewerkt. Via verschillende overlegstructuren hebben we veel mogelijkheden om onze zienswijze in goede discussies met de overheid te bespreken. Er is een sterk gevoel van een gemeenschappelijk belang bij zowel overheid als private partijen. Deze intensieve samenwerking kan soms een nadeel zijn aangezien men tendeert naar een compromis in plaats van het maken van scherpe keuzes over wat nu vitaal is voor de nationale veiligheid.
In Duitsland merken we een grotere afstand tussen overheid en bedrijfsleven. Ook tussen de vitale private partijen is samenwerking en informatie-uitwisseling minder vanzelfsprekend dan in Nederland. Dit heeft ongetwijfeld met de schaalgrootte van Duitsland te maken, maar ook met een traditie dat men meer geneigd is om afspraken in wetgeving vast te leggen. Een mooi voorbeeld is de Europese richtlijn over de bescherming van Europese Critical Infrastructure; in Nederland is deze omgezet in beleidsaanpassingen, in Duitsland is dat nauw omschreven in wetgeving. In Duitsland vindt nu een discussie met de vier TSO's plaats over wat exact van vitaal belang is voor de nationale veiligheid. We zien dat de Duitse overheid kritischer is om te bepalen wat nu echt tot de vitale infrastructuur behoort."

4. WAT ZIJN DE GROOTSTE UITDAGINGEN DE KOMENDE 5-10 JAAR VOOR DE WEERBAARHEID VAN DE VITALE PROCESSEN, WAARBIJ TENNET IS BETROKKEN?

"De toenemende hyperconnectiviteit zorgt voor een toename van onderlinge afhankelijkheden. Grote storingen bij andere vitale partners kunnen TenneT meer en meer raken. Daarnaast is er de maatschappelijke ontwikkeling dat we geen enkele verstoring van het dagelijks leven meer accepteren. Door de zeer hoge betrouwbaarheid van 99,99% van ons net ontstaat het idee dat er nooit iets fout kan gaan. De stroomstoring die op 27 maart jl. Amsterdam en een deel van Noord/Holland en Flevoland raakte, zorgt dat de discussie over leveringszekerheid versus efficiënt investeren in ons elektriciteitsnet weer oplaait. Daarnaast heeft ook TenneT in toenemende mate te maken met steeds sneller veranderende nieuwe dreigingen op het gebied van cybersecurity waartegen wij ons steeds moeten blijven wapenen. Er is altijd een spanningsveld tussen de hoeveelheid investeringen en het risico dat je als vitale organisatie mag en wil lopen."