2de inhoudelijke analyse
bescherming vitale infrastructuur

Inhoudsopgave

1 Inleiding

In 2005 is voor het eerst een inhoudelijke analyse over de bescherming van de vitale infrastructuur in Nederland aan de Tweede Kamer aangeboden[1]. Er is toen toegezegd om dit in 2009 te herhalen. Tussen 2005 en 2009 zijn mede op basis van de analyse uit 2005 belangrijke stappen gezet om de bescherming van de vitale producten en diensten te versterken (Hierover is eerder gerapporteerd)[2]. Dit is door een intensieve samenwerking tussen publieke en private partijen tot stand gebracht. Het heeft er toe geleid dat de bescherming van de vitale infrastructuur in Nederland op een adequate manier wordt aangepakt. In het vervolg wordt beschreven hoe dit tot stand is gekomen.

2 Aanpak

Om te komen tot een uitspraak over hoe het anno 2009 gesteld is met de bescherming van de vitale infrastructuur in Nederland is gebruik gemaakt van een aantal te beantwoorden hoofdvragen. Deze vragen zijn ook in 2005 leidend geweest bij de destijds opgestelde analyse over de bescherming van vitale infrastructuur.

Op de eerste plaats moet vastgesteld worden wat we in Nederland zien als vitale infrastructuur, welke producten, diensten en processen hierbij van belang zijn en nog concreter of hierbij specifieke elementen c.q. objecten zijn aan te wijzen.

Op de tweede plaats is bekeken welke dreigingen daadwerkelijk van invloed zijn op het functioneren van deze vitale producten, diensten en processen. In 2005 is hiervoor een lijst met zogenaamde begingebeurtenissen opgesteld. In de afgelopen jaren is met de introductie van de strategie Nationale Veiligheid en de samenwerking op het terrein van o.m. terrorisme het inzicht hierin sterk verbeterd en wordt juist met informatie uit deze trajecten gewerkt. Hierbij gaat het onder meer om de dreigingscenario's die ten behoeve van de Nationale Risicobeoordeling zijn opgesteld.

Op de derde plaats wordt bekeken of de huidige situatie, met de genomen maatregelen, maar ook gerealiseerde samenwerkingsverbanden en kennis- en informatie-uitwisseling naar verwachting voldoende zal zijn om een mogelijke bedreiging, dan wel uitval van een vitaal product, dienst of proces het hoofd te bieden.
Hierbij wordt van de filosofie uitgegaan dat de mate waarin de vitale producten, diensten en processen in Nederland afdoende beschermd kunnen worden bepaald wordt door:

1. Weten wie wat moet doen: heldere verantwoordelijkheden.
2. Weten welke dreigingen er spelen: structureel inzicht.
3. Weten met wie samen te werken en dit ook doen: actieve netwerken.
4. Samen voorbereid zijn op mogelijke uitval.

Als laatste vraag wordt beantwoord welke acties er nog de komende tijd ondernomen moeten worden en hoe de aandacht voor de bescherming van de vitale infrastructuur bij alle betrokken partijen ook in de toekomst op het goede niveau blijft.

---

[1] Tweede kamer, vergaderjaar 2005-2006, 26643 nr. 75

[2] Tweede Kamer, vergaderjaar 2006-2007, 26643 nr. 83, vergaderjaar 2007-2008 29668 nr. 18, vergaderjaar 2008-2009, 29668 nr. 26.

De antwoorden op deze vragen zijn afgeleid uit verschillende activiteiten en onderzoeken die de afgelopen jaren zowel in individuele vitale sectoren als in samenwerking tussen meerdere sectoren en overheden (intersectoraal) zijn uitgevoerd. Met het beantwoorden van deze vragen wordt het mogelijk antwoord te geven op de vraag hoe het gesteld is met de bescherming van vitale infrastructuur.

3 Wat is vitale infrastructuur (en welke partijen zijn daarbij betrokken)?

Om de vitale infrastructuur adequaat te beschermen is het ten eerste van belang om te weten wat het is en welke partijen betrokken zijn. Vitale infrastructuren zijn die producten, diensten en processen die, als zij uitvallen, maatschappelijke of economische ontwrichting van (inter-)nationale omvang kunnen veroorzaken, doordat er veel slachtoffers kunnen vallen en/of omdat het herstel zeer lang gaat duren en er geen reële alternatieven voorhanden zijn, terwijl we deze producten en diensten niet kunnen missen. Omdat de gevolgen van de uitval van (delen van de) vitale infrastructuur voor grote delen van de Nederlandse samenleving zeer ernstig kunnen zijn, vergt de bescherming daarvan extra aandacht. Overigens blijft hierbij gelden dat honderd procent veiligheid niet te realiseren is en dat naast bescherming, het voorbereid zijn op mogelijke uitval door overheid, bedrijfsleven en burger gedegen aandacht vergt.

In 2004 is er een indeling op hoofdlijnen gemaakt bestaande uit twaalf vitale sectoren. Op basis hiervan is in 2005 de eerste inhoudelijke analyse uitgevoerd, waarbij per sector onder meer is nagegaan welke producten en diensten vitaal zijn voor het functioneren van de maatschappij. Dit heeft in 2005 geleidt tot een lijst van uiteindelijk 33 producten en diensten welke als vitaal product en dienst zijn benoemd. Per sector is daarbij bepaald welke elementen c.q. objecten exact kritiek zijn voor deze producten, diensten en processen.

In 2008 is op basis van vervolgonderzoek een aantal producten en diensten als randvoorwaardelijk betiteld voor alle anderen. Deze randvoorwaardelijke sectoren zijn:

- Elektriciteit, aangezien alle vitale producten en diensten hiervan afhankelijk zijn;
- Gas, aangezien vooral de elektriciteitssector hier sterk van afhankelijk is en deze, gezien het bovenstaande, weer veel effect op andere sectoren heeft;
- Drinkwater, aangezien mens en dier maar heel kort zonder kunnen;
- Telecom/ICT, aangezien een zeer groot deel van de huidige technische systemen vervlochten zijn met telecom- en ICT verbindingen;
- Keren en beheren oppervlaktewater, aangezien grootschalige overstromingen desastreus zijn voor de samenleving en voor de vitale infrastructuur in Nederland;
- (weg) transport tijdens crisissituaties, aangezien bijna alle vitale sectoren in sterke mate afhankelijk zijn van aan en afvoer van producten en diensten.

Deze typering als randvoorwaardelijk is voortgekomen uit een analyse van de grootste afhankelijkheidsrelaties en had prioritering in het kader van voorbereiding op crisis en rampen door onder meer de veiligheidsregio's tot doel.

Op hoofdlijnen is de indeling zoals die in 2005 is vastgesteld, op dit moment nog steeds relevant. Hieronder is het overzicht van alle vitale sectoren, producten en diensten per 2009 opgenomen. Hierbij dient te worden opgemerkt dat waar voor het merendeel van de vitale producten en diensten geldt dat deze in de loop van de tijd niet snel zullen veranderen, dit niet in alle gevallen zo zal zijn. Op het niveau van wat nu precies de vitale

elementen c.q. objecten binnen een sector zijn geldt dit gegeven nog sterker. In de loop van de tijd kunnen door ontwikkelingen binnen de sector, maar juist ook door veranderde dreigingen of afhankelijkheden andere specifieke zaken vitaal worden binnen de algemene context van een vitaal product of dienst. Uitzondering op de relatief langzame veranderingen is te vinden binnen de sector Telecom/ICT. De grootschalige innovaties en ontwikkelingen die juist binnen deze sector plaats vinden en die onze maatschappij in de afgelopen jaren allerlei nieuwe mogelijkheden van onder meer communicatie- en informatie-uitwisseling hebben gebracht, leiden er onder meer toe dat satellietcommunicatie en de post- en koeriersdiensten op dit moment niet langer als vitaal aangemerkt hoeven te worden. Uitgaande van het feit dat veranderingen wel altijd mogelijk zijn, is het van groot belang om continu aandacht te besteden als sectorpartijen en overheden aan welke zaken nu als vitaal gezien kunnen worden. Dit proces kan niet beperkt worden tot eens in de vier jaar, maar hoort onderdeel te zijn van lopende processen. Onder meer in de financiële en ICT/Telecom sector loopt zelfs op dit moment weer een herijking op dit vlak.

Sector	**Product of dienst**
1) Energie	1. elektriciteit 2. aardgas 3. olie
2) Telecommunicatie/ ICT	4. vaste telecommunicatie-voorziening 5. mobiele telecommunicatie-voorziening 6. radiocommunicatie en navigatie 7. omroep (crisiscommunicatie) 8. internettoegang
3) Drinkwater	9. drinkwatervoorziening
4) Voedsel	10. voedselvoorziening/ -veiligheid
5) Gezondheid	11. spoedeisende zorg/ overige ziekenhuiszorg 12. geneesmiddelen 13. sera en vaccins 14. nucleaire geneeskunde
6) Financieel	15. betalingsdiensten/ betalingstructuur 16. financiële overdracht overheid
7) Keren en Beheren oppervlaktewater	17. beheren waterkwaliteit 18. keren en beheren waterkwantiteit
8) Openbare Orde en Veiligheid	19. handhaving openbare orde 20. handhaving openbare veiligheid
9) Rechtsorde	21. rechtspleging en detentie 22. rechtshandhaving
10) Openbaar bestuur	23. diplomatieke communicatie 24. informatieverstrekking overheid 25. krijgsmacht 26. besluitvorming openbaar bestuur
11) Transport	27. mainport Schiphol 28. mainport Rotterdam 29. hoofdwegen- en hoofdvaarwegennet

Sector	Product of dienst
	(Rijksinfrastructuur) 30. spoorsysteem
12) Chemische en Nucleaire industrie	31. vervoer, opslag en productie/verwerking van chemische en nucleaire stoffen

Betrokken partijen: 'Partners in veiligheid'
Bij de bescherming van de vitale infrastructuur zijn een groot aantal partijen betrokken. Deze partijen zijn binnen Nederland op hoofdlijnen in te delen in de volgende categorieën:

- eigenaren en beheerders van de vitale infrastructuur (privaat en publiek);
- medeoverheden, waaronder politie- en veiligheidsregio's.;
- nationale overheid.

Deze partijen kennen allemaal hun eigen verantwoordelijkheden en spelen vanuit die verantwoordelijkheid een bepaalde rol bij dit onderwerp.

Eigenaren en beheerders van vitale producten, diensten en processen zijn op de eerste plaats verantwoordelijk om hun eigen bedrijfscontinuïteit te waarborgen.

Medeoverheden zijn verantwoordelijk voor de openbare orde en veiligheid en voor crisisbeheersing op hun grondgebied. Hierbij is samenwerking met eigenaren en beheerders van vitale infrastructuur van groot belang onder meer om goed voorbereidt te zijn op aantasting- en uitval van de betreffende vitale producten en diensten.

De nationale overheid ondersteunt beide partijen door kennis en informatie uit te (laten) wisselen en door alle partijen samen te brengen op sectoroverstijgende thema's zoals afhankelijkheden. In een crisissituatie is de nationale crisisorganisatie verder verantwoordelijk voor de respons op nationaal niveau.
De verantwoordelijkheid binnen de nationale overheid is opgedeeld in vakministeries die op nationaal niveau verantwoordelijk zijn voor één of twee sectoren. Het ministerie van BZK voert de regie over het thema nationale veiligheid en daarmee ook het thema bescherming vitale infrastructuur als geheel.

Naast de boven beschreven partijen die een belangrijke rol in de Nederlandse context spelen, geldt dat vitale infrastructuur in steeds grotere mate een grensoverschrijdend karakter heeft. Veel vitale producten, diensten en processen kennen grens overschrijdende relaties zowel fysiek als organisatorisch. Daarnaast geldt dat ook veel leveranciers of afnemers in het buitenland zitten. De grote internationale betekenis van vitale infrastructuur is ook de reden dat sinds een aantal jaar de Europese Commissie zich intensief bezig houdt met het onderwerp en er sinds begin 2009 een richtlijn op dit terrein van kracht is.

4 Relevante dreigingen

Wetende wat de vitale producten, diensten en processen zijn, moeten de betrokken partijen zich bewust zijn van de mogelijke dreigingen die op Nederland afkomen en die relevant kunnen zijn voor het functioneren van de betreffende vitale onderdelen. Om (mogelijk) maatregelen te kunnen nemen moeten zij de dreigingen op waarde kunnen

schatten en een beeld hebben van hun afhankelijkheden van ketenpartners of crisisorganisaties. Hiervoor is een "all-hazard" benadering het uitgangspunt. Dit houdt in dat elk soort dreiging dat relevant zou kunnen zijn moet worden meegenomen bij heb bepalen van de mate waarin de bescherming van de vitale producten, diensten en processen is geregeld. Hierbij kan het gaan om dreigingen met een natuurlijke oorzaak, zoals overstromingen, maar ook om technisch of organisatorisch falen of dreigingen die voortkomen uit het al dan niet opzettelijk handelen van mensen. Bij deze laatste categorie - het opzettelijk handelen- is er natuurlijk extra aandacht voor mogelijk terroristisch handelen.

In de afgelopen jaren zijn verschillende analyses en onderzoeken gedaan om de betekenis van allerlei dreigingen voor het functioneren van de vitale infrastructuur nader in kaart te brengen en te bepalen hoe kwetsbaar de verschillende vitale producten, diensten en processen zijn voor deze dreigingen.
Uit deze brede benadering is gebleken dat er een aantal dreigingtypen is dat voor het merendeel van de vitale sectoren relevant is. Hierbij gaat het om overstroming, grieppandemie, elektriciteit- en ICT-uitval en moedwillige verstoring (security). Dit wordt onder meer onderschreven in de uitkomsten van de Nationale Risicobeoordeling (NRB) (TK 2008-2009, 30821, nr. 8), waarbij deze dreigingen als significant voor het functioneren van de Nederlandse maatschappij naar voren komen.
Het feit dat er een aantal duidelijk aanwijsbare dreigingen is dat voor alle vitale sectoren relevant is wil niet zeggen dat hiermee alle relevante dreigingen benoemd zijn. Per sector bestaat ook zicht op dreigingen die vanwege specifieke kenmerken van het betreffende vitale product, dienst of proces relevant kunnen zijn.

Afhankelijkheden
Het inzicht in de betekenis van deze dreigingen voor de vitale sectoren heeft geleidt tot concrete acties om juist de weerbaarheid tegen een aantal van deze dreigingen te versterken. Zo is bij de voorbereiding op een mogelijke overstroming onderleiding van de Taskforce Management Overstromingen (TMO) in de periode 2007-2008 in heel Nederland veel aandacht geweest voor de betrokkenheid en bescherming van vitale infrastructuur. Bij de voorbereiding op grieppandemie in de periode 2008-2009, waarover een aparte rapportage is opgesteld, is de continuïteit van vitale infrastructuur één van de belangrijkste aandachtsgebieden. Op dit moment loopt nog een traject om tot eind 2010 de weerbaarheid van alle vitale sectoren tegen uitval van ICT/Telecom en elektriciteit verder te versterken.
Bij deze activiteiten heeft de toegenomen kennis over de betekenis van afhankelijkheden tussen verschillende vitale sectoren een belangrijke rol gespeeld. Dit aandachtspunt uit de analyse 2005 heeft in de afgelopen jaren een dominante rol gespeeld bij de totstandkoming van netwerken, de uitvoering van analyses en het nemen van maatregelen. De kennis over welke afhankelijkheden er zijn en wat deze kunnen betekenen voor de verschillende partijen binnen het netwerk van vitale infrastructuren is sinds 2005 sterk toegenomen. Het Strategisch Overleg Vitale Infrastructuur (SOVI), dat naar aanleiding van de analyse uit 2005 in 2006 is opgericht om het contact tussen de vitale sectoren onderling te versterken, heeft een aantal onderzoeken uitgevoerd naar specifieke afhankelijkheidsrelaties op het terrein van elektriciteit en ICT. Ook is met behulp van de dreigingsscenario's die speciaal voor de Nationale Risicobeoordeling (NRB) zijn ontwikkeld bekeken wat deze dreigingen voor de afhankelijkheidsrelaties van vitale sectoren onderling en van deze organisaties met de overheid, betekent. Deze analyses

hebben ondermeer geleidt tot een scherper beeld van welke producten en diensten als randvoorwaardelijk te betitelen zijn voor het functioneren van alle vitale sectoren. Verder heeft het er voor gezorgd dat sinds 2005 de behoefte aan informatie-uitwisseling tussen vitale sectoren onderdeling sterk is toegenomen. Dit vindt in toenemende mate plaats via allerlei al dan niet formele overlegstructuren. Deze worden ondermeer ondersteund door organisatie(vormen) als het Nationale Adviescentrum Vitale Infrastructuur (NAVI) en het programma Nationale Infrastructuur Cybercrime (NICC). Zie ook hoofdstuk 5.

Geconcludeerd kan worden dat er grote stappen gemaakt zijn, maar dat de complexiteit van het afhankelijkheidsvraagstuk leidt tot de behoefte om blijvend aandacht aan dit vraagstuk te besteden. De dynamiek van sectoren, netwerken, partijen en dreigingen geven hier ook aanleiding toe.

Moedwillige verstoring en terrorisme
Moedwillige verstoring en met name terrorisme blijft een dreiging die voor alle sectoren relevant is. Dit komt naar voren uit de vele analyses die de afgelopen jaren zijn uitgevoerd op dit terrein. Hierbij gaat het duidelijk niet alleen om de kans van optreden, maar juist ook om de potentiële effecten die zo'n dreiging met zich mee kan brengen. Het gedegen voorbereidt zijn op moedwillige verstoring en het wanneer nodig kunnen optreden mocht zo'n dreiging zich voordoen is van groot belang. Op het terrein van moedwillige verstoringen en specifiek terrorisme is sinds 2005 de uitwisseling van informatie over dreigingen tussen overheidspartijen en vitale sectoren dan ook sterk verbeterd. In algemene zin is de kennis op dit terrein vergroot doordat o.m. het Nationaal Adviescentrum Vitale Infrastructuur (NAVI) en de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) informatie over relevante dreigingen uitwisselen met de vitale sectoren. Daarnaast zijn sinds 2005 het merendeel van de vitale sectoren aangesloten op het Alerteringssysteem Terrorismebestrijding (ATb). Hierdoor krijgen deze partijen via de Nationale Coördinator Terrorismebestrijding (NCTb) informatie over specifieke (mogelijke) terroristische dreigingen.
Op basis van deze informatie is het voor de verschillende vitale partijen nu beter mogelijk in te schatten of de bescherming tegen deze dreigingen nu afdoende is.

5 Hoe is de vitale infrastructuur beschermd?

Zoals in de analyse van 2005 ook al naar voren kwam is de bescherming van vitale infrastructuur niet alleen afhankelijk van concreet genomen maatregelen, maar juist ook van een gedegen en structurele kennis over de dreigingen die kunnen optreden, de mogelijke handelingen die hier tegen kunnen worden ondernomen en de netwerken van partijen die hierbij een rol spelen. Sinds 2005 is dan ook niet alleen ingezet op het nemen van concrete maatregelen binnen en tussen sectoren, maar juist ook op het vergroten van de kennis over dreigingen, over afhankelijkheden en over betrokken partijen.

Concreet kan gesteld worden dat de mate waarin de vitale producten, diensten en processen in Nederland afdoende beschermd kunnen worden bepaald wordt door:

1. Weten wie wat moet doen: heldere verantwoordelijkheden
2. Weten welke dreigingen er spelen: structureel inzicht
3. Weten met wie samen te werken en dit ook doen: actieve netwerken
4. Samen voorbereid zijn op mogelijke uitval

Naast deze hoofdthema's zijn er ook nog een aantal punten die onder meer in 2005 als zeer relevant naar voren zijn gekomen. Hierbij gaat het om de vraagstukken 'security (moedwillige verstoring)', internationale ontwikkelingen en oefenen. Hieronder wordt eerst beschreven hoe het met de hoofdthema's is gesteld, daarna wordt ingegaan op deze concrete punten.

1. Weten wie wat moet doen: heldere verantwoordelijkheden

Om tot een adequaat beschermingsniveau te komen is het van cruciaal belang dat duidelijk is wat ieders verantwoordelijkheden zijn en wat de partijen van elkaar kunnen verwachten. De intensieve samenwerking, sterke betrokkenheid en concrete acties zoals die in de afgelopen jaren hebben plaats gevonden en nog steeds gaande zijn leiden tot de conclusie dat alle betrokken partijen in de afgelopen jaren doordrongen zijn van hun verantwoordelijkheid en deze ook nemen.
De uitwerking van deze verantwoordelijkheden zoals ook in hoofdstuk 3 op hoofdlijnen beschreven zijn voor bepaalde sectoren al in wet en regelgeving vastgelegd. Het concept van 'goed huisvaderschap', dat door de drinkwatersector is geconcretiseerd naar specifieke taken en normen wordt in het nieuwe drinkwaterbesluit, dat naar verwachting op 1 januari 2011 van kracht wordt, opgenomen. Ook voor sectoren als energie, telecom/ICT en Openbare Orde en Veiligheid geldt dat er afspraken worden gemaakt over de verantwoordelijkheden en met name hoe deze verantwoordelijkheden worden ingevuld in concrete termen als kwaliteit van de dienstverlening.

Verder blijkt uit de manier waarop het overgrote deel van de partijen binnen de verschillende vitale sectoren continuïteitsplannen in het kader van grieppandemie hebben opgesteld, dat men zich terdege bewust is van de eigen verantwoordelijkheid voor de continuïteit van dienstverlening.

2. Weten welke dreigingen er spelen: structureel inzicht

Zoals ook in hoofdstuk 3 en 4 beschreven is er in de afgelopen jaren door de intensieve samenwerking en met zaken als de strategie nationale veiligheid en de concrete uitwisseling van dreiginginformatie een situatie ontstaan, waarbij het inzicht in welke elementen precies vitaal zijn, welke dreigingen relevant zijn en wat dit betekend voor de continuïteit van vitale producten, diensten en processen sterk is toegenomen.
Er is nu sprake van een situatie, waarbij systematisch informatie kan worden uitgewisseld en gezamenlijk bepaald kan worden wat de betekenis van deze dreigingen zou kunnen zijn.
Uit de recente voorbereiding op de grieppandemie die voort is gekomen uit de NRB 2008 blijkt al dat deze manier van werken ook daadwerkelijk effectief kan zijn. Ook op het terrein van ICT/Telecom en elektriciteitsuitval is op basis van de verschillende analyses van onder meer het SOVI en de NRB 2008-2009 nu bepaald dat er een extra actie nodig is om de weerbaarheid van vitale infrastructuren te versterken. Daarbij wordt gebruik gemaakt van de kennis over kwetsbaarheden en afhankelijkheden die er over de jaren is opgedaan en doorgepakt op de vele maatregelen die al zijn genomen. Bovendien wordt de nationale respons op uitval van ICT/Telecom diensten en op uitval van elektriciteit versterkt.

3. Weten met wie samen te werken en dit ook doen: actieve netwerken

Kennis over welke partijen allemaal betrokken zijn bij het vraagstuk bescherming vitale infrastructuur zowel binnen andere sectoren als bij de overheid was in 2005 één van de zorgpunten, die nadere aandacht behoefde.
Sinds 2005 is structureel aandacht besteed aan het samenbrengen van alle partijen. Dit gebeurde ondermeer via allerlei werkgroepen op meer operationeel niveau rond thema's als dreigingen en afhankelijkheden, maar is ook gedaan middels meer formele overleggen zoals het Strategisch Overleg Vitale Infrastructuur (SOVI) en de commissie vitaal van VNO-NCW.
Ook binnen sectoren is de samenwerking verder gestructureerd, zo kent de Telecomsector een formeel overleg (Nationaal Coördinatie Overleg-Telecom NCO-T) dat zich bezig houdt met de kwaliteit van dienstverlening en is in de financiële sector sinds 2009 het netwerk uitgebreid met een Platform Business Continuity Vitale Infrastructuur (BC VIF).

Verder is afgesproken dat alle betrokken ministeries verantwoordelijk zijn om de partijen binnen 'hun' vitale sector te informeren en te betrekken bij ontwikkelingen op het terrein van de Nationale Veiligheid. Voor alle sectoren geldt dan ook dat er (specifieke) netwerken bestaan waar onderwerpen op het terrein van continuïteit van dienstverlening en bescherming van vitale infrastructuur kunnen worden besproken.

4. Samen voorbereid zijn op mogelijke uitval

Naast het voorkomen van uitval van vitale infrastructuur is in vergelijking tot de situatie in 2005 in de afgelopen jaren het belang van goed voorbereid zijn op een mogelijke aantasting of uitval steeds belangrijker geworden. Incidenten van een kleinere schaal, zoals de uitval van elektriciteit in Haaksbergen en de Bommelerwaard, maar ook verschillende verstoringen van de telecommunicatie en drinkwatervoorziening hebben hieraan bijgedragen. Ook is er uit deze incidenten veel waardevolle informatie gekomen over onder meer de samenwerking tussen overheid en veiligheidspartners zoals vitale organisaties. In de afgelopen jaren is dan ook sterk ingezet op het kunnen beheersen van mogelijke uitval van vitale producten, diensten en processen. Hierbij spelen met name ook veiligheid's- en politieregio's naast de beheerders van vitale infrastructuren een belangrijke rol.

De minister van BZK heeft in 2007 en 2008 met een groot aantal veiligheidsregio's convenanten gesloten waarin onder andere vitale infrastructuur als aandachtsgebied is benoemd. In 2008 zijn de burgemeesters en de voorzitters van de veiligheidsregio's vertrouwelijk geïnformeerd door de minister van BZK over de vitale objecten op hun grondgebied om zo samen met de beheerders van deze objecten de voorbereiding op mogelijke uitval van vitale producten of diensten aan te kunnen pakken. In vergelijking met 2005 zijn de vitale sectoren, medeoverheden en nationale overheid nu nog beter geïnformeerd. Hierdoor zijn zij beter in staat om waar nodig handelend op te treden en maatregelen te treffen voor adequate bescherming.
In vervolg hierop zijn mede op initiatief van de drinkwatersector er recent convenanten gesloten tussen veiligheidsregio's en de drinkwatersector over gezamenlijke voorbereiding op uitval van dienstverlening en samenwerking in crisissituaties. Het Veiligheidsberaad heeft het voortouw genomen om soortgelijke convenanten te laten ontwikkelen tussen de landelijk georganiseerde vitale sectoren (elektriciteit, drinkwater, gas en Telecom) en de veiligheidsregio's. Dit zal leiden tot een betere samenwerking op regionaal niveau tussen vitale infrastructuur en veiligheidsregio's.

Op nationaal niveau is de samenwerking met het bedrijfsleven structureel belegd onder meer doordat VNO-NCW deelneemt aan de interdepartementale stuurgroep nationale veiligheid en de nationale crisisorganisatie. Op topniveau hebben de minister van BZK en de voorzitter van VNO-NCW ook afspraken gemaakt over samenwerking. Eén van deze afspraken is dat de overheid één loket biedt aan het bedrijfsleven. Ten tijde van crisis kunnen bedrijven nu ook terecht bij het Nationaal Crisiscentrum voor informatie naast de lijn met het eigen vakministerie.

Om informatievoorziening tijdens crisissituaties zo goed mogelijk te laten functioneren is in de afgelopen periode onder meer gewerkt aan de noodcommunicatie. Op basis van de analyse van 2005 is een traject ingezet om naar mogelijke opvolging van het Nationale Noodnet (NN) te kijken. De vitale sectoren hebben unaniem aangeven dat dit een noodzakelijke voorziening is die opvolging moet krijgen. Inmiddels is een contract getekend met KPN voor de opvolger van het Noodnet, de zogenaamde Noodcommunicatievoorziening (NCV). Het NCV zorgt ervoor dat bij verstoringen van de openbare voorzieningen toch nog communicatie mogelijk is tussen overheidsorganisaties onderling en met het vitale bedrijfsleven. Juist omdat het een "last resort" communicatievoorziening is, wordt er net als bij het eerdere Noodnet veel aandacht besteed aan de betrouwbaarheid en weerbaarheid tegen fysieke en niet fysieke dreigingen. Zo blijft het nieuwe netwerk beschikbaar als het gewone vaste telefoonverkeer tijdens een ramp uitvalt door overbelasting of stroomuitval. Zelfs het gebruik van mobiele telefoons is mogelijk wanneer het gewone gsm-verkeer door overbelasting uitvalt.

Security, moedwillige verstoring
Een ander thema waarin veel bereikt is sinds 2005 is het thema security. In 2005 is geconcludeerd dat er meer inzet nodig was om vitale sectoren te beveiligen tegen moedwillige verstoring. Meerdere initiatieven zijn succesvol ontplooid om te komen tot de huidige stand van beveiliging. Zo is door middel van convenanten met de (petro-)chemische industrie over beveiligingsmaatregelen, zoals de invoering van een security management systeem (SMS), het veiligheidsniveau verhoogd. In de mainport Rotterdam is voor de hele haven een beveiligingsplan gerealiseerd. Dit Port Security Plan dat is opgesteld op basis van de Europese Richtlijn Havenbeveiliging, is tot stand gekomen door intensieve samenwerking van alle partijen in het havengebied.
De samenwerking met de politieregio's in algemene zin is ook versterkt doordat vitale sectoren zich hebben aangesloten bij het Alerteringsysteem Terrorismebestrijding (ATb) van de Nationaal Coördinator Terrorismebestrijding (NCTb). Om de samenwerking op het gebied van security te stimuleren is in 2007 het Nationaal Adviescentrum Vitale Infrastructuur (NAVI) opgericht. NAVI ondersteunt het bedrijfsleven met advies over securityvraagstukken en biedt een platform waar veiligheidspartners samenkomen. In twee jaar tijd heeft NAVI veel bijgedragen aan de bewustwording over security. Zo heeft NAVI een aantal risicoanalyses uitgevoerd over onder andere de beveiliging van buisleidingen en de gevolgen van ICT-uitval. De Nationale Infrastructuur ter bestrijding van Cybercrime (NICC) biedt ook een platform voor publieke en private partners op het meer specifieke gebied van cybercrime. Sinds 2005 is gebleken dat cybercrime een belangrijk thema is waar in de toekomst meer op moet worden ingezet. Gezien dit vergroot belang is een krachtenbundeling in gang gezet van NAVI, NICC en GOVCERT. Deze samenvoeging zal in 2010 verder vorm krijgen.

Een laatste belangrijke ontwikkeling die in 2009 in gang gezet is door de Nationaal Coördinator Terrorismebestrijding (NCTb) zijn de zogenaamde security awareness workshops 'Zeker van je Zaak.' Hiermee helpt de NCTb bedrijven en instellingen bij het versterken van security awareness op de werkvloer door het aanreiken van praktische instrumenten en informatie. Het doel is het bewustzijn van medewerkers van deze bedrijven en instellingen te vergroten en daardoor te voorkomen dat verstoringen van de bedrijfsvoering plaatsvinden door acties van criminelen, vandalen, extremisten en terroristen. De aangereikte kennis en handelingsperspectieven worden vervolgens door deze partijen in eigen opleidingen gebruikt.

Internationale ontwikkelingen

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 op dit terrein goed vertegenwoordigd in Europa en daarbuiten. In Europa geldt dat Nederland zelfs één van de koplopers is. Sinds begin 2009 is de Europese richtlijn voor vitale infrastructuur van kracht[3]. Doel van deze richtlijn is de bepaling van Europese vitale infrastructuur, welke vervolgens onder meer security management systemen moeten invoeren. Nederland heeft de implementatie van deze richtlijn voortvarend opgepakt en heeft onder meer sinds begin 2009 een zogenaamd CIP contactpoint Nederland ingesteld. Hier binnen werken de zes meest betrokken ministeries intensief samen om de implementatie van de EPCIP richtlijn uit te voeren. Verder is er internationaal intensieve samenwerking met andere landen ook waar het gaat om specifieke thema's als het in kaart brengen van dreigingen en samenwerking met kennisinstituten. Op het gebied van ICT heeft de EU recent een apart CIIP programma (critical information infrastructure program) opgezet, dat onder meer tot doel heeft criteria voor ICT infrastructuur in het kader van EPCIP richtlijn te definiëren.

Zorgen dat het werkt: oefenen

Wanneer alle bovenstaande elementen samenkomen is het de vraag of het werkt. Om dit te garanderen is het belangrijk dat er wordt geoefend. Hierbij wordt steeds intensiever samengewerkt tussen overheden en vitale organisaties. Onder andere bij de landelijke oefeningen Waterproef en Voyager in 2008 en 2007 zijn vitale sectoren intensief betrokken geweest. Ook internationaal wordt veel geoefend tussen overheden en vitale partijen zo als bijvoorbeeld tijdens de Emergency Response Exercise 4 van het Internationale Energie Agentschap (IEA). Ook in 2010 zullen verschillende Nederlandse partijen betrokken zijn bij een grote internationale oefening (Cyberstorm III), waarbij aantasting van ICT systemen beoefend wordt.

Meer specifiek zijn in het kader van het Alerteringssysteem Terrorismebestrijding in de afgelopen jaren een groot aantal oefeningen gehouden. Door dat de relaties tussen vitale partijen en overheidsdiensten op het gebied van rampen en crisisbeheersing steeds hechter worden, wordt er ook steeds meer op regionaal en sectorniveau multidisciplinair geoefend. Hiermee wordt er aan bijgedragen dat de getroffen maatregelen in echte noodsituaties ook daadwerkelijk werken. Naast samenwerking tussen overheden en vitale organisaties gaat ook steeds meer aandacht uit naar de zelfredzaamheid van burgers. De 'denk vooruit'-campagne is een goed voorbeeld van de inzet om het bewustzijn rond

[3] Tweede Kamer, vergaderjaar 2008-2009, 22112 nr. 793

zelfredzaamheid te vergroten. Niet alleen het alarmeren van burgers, maar vooral het bieden van handelingsperspectieven is bij zelfredzaamheid een belangrijk thema. Burgers worden dan ook via de 'denk vooruit'-campagne direct aangesproken op het zelf voorbereidt zijn op uitval van vitale producten en diensten, zoals drinkwater, elektriciteit en communicatievoorzieningen.

6 Uitdagingen voor de toekomst

De samenleving is voortdurend in ontwikkeling. Dit betekent dat de vitale sectoren, producten en diensten ook continue in ontwikkeling zijn. Aandacht voor het onderwerp moet dan ook onderdeel uitmaken van de reguliere processen van overheid en bedrijfsleven. Vergeleken met 2005 is het onderwerp onderdeel geworden van de reguliere processen van alle veiligheidspartners, maar de aandacht moet ook in de toekomst worden vastgehouden. Er moet continue inzicht blijven bestaan bij alle veiligheidspartners in de stand van de bescherming, vooral in snel ontwikkelende sectoren zoals Telecom en ICT. Er zijn veel samenwerkingsafspraken gemaakt tussen veiligheidspartners en deze lopende afspraken moeten in de aankomende jaren worden bestendigd. Belangrijke elementen hierbij zijn:

- de weerbaarheid van de vitale infrastructuur bij uitval van elektriciteit en ICT,
- de landelijke samenwerkingsafspraken tussen de vitale sectoren en het Veiligheidsberaad
- de krachtenbundeling van NAVI, GOVCERT en NICC.

Internationaal zal de implementatie van de EPCIP-richtlijn in 2011 afgerond worden. In het kader van het bredere EPCIP-programma zal Nederland nauw betrokken blijven bij nieuwe voorstellen van de Europese Commissie. Nederland zal zich blijven inzetten voor intensieve samenwerking met andere landen en kennisinstituten.

Sinds het ontstaan van de Strategie Nationale Veiligheid zijn grote stappen gezet om dreigingen te identificeren en te beoordelen, om belangrijke capaciteiten te identificeren en om in de beleidsopvolging de samenleving meer weerbaar te maken. De grootschalige voorbereidingen op een mogelijke grieppandemie in 2008 en 2009 door overheden en bedrijfsleven (waaronder de vitale organisaties) zijn een goed voorbeeld hiervan. Een uitdaging voor de toekomst is om de impact van dreigingen op de kwetsbaarheid van vitale infrastructuur verder te integreren in de Strategie Nationale Veiligheid. Het streven is om vierjaarlijks een verdieping van de Nationale Risicobeoordeling en bijbehorende capaciteitenanalyse plaats te laten vinden die inzoomt op de vitale infrastructuur. Hiermee wordt vervolg gegeven aan de toezegging aan de Tweede Kamer om elke vier jaar integraal te rapporteren over de stand van de bescherming van de vitale infrastructuur.

Bijlage: samenvatting per sector

1 Sector Energie

Typering sector:
Zekerheid omtrent de voorziening van energie is voor de maatschappij van groot belang. Vrijwel alle vitale producten en diensten hebben een hoge mate van afhankelijkheid van elektriciteit, olie en gas. Dit geldt zowel nationaal als internationaal, waar zowel Nederland afhankelijk is van het buitenland als het buitenland afhankelijk is van Nederland om te voorzien in een continue aanlevering van energie.

Netwerk en verantwoordelijkheidsverdeling:

- Transport over en beheer van het elektriciteitsnetwerk zijn tegenwoordig losgekoppeld van de productie van elektriciteit. Het (hoogspannings-)elektriciteitsnetwerk wordt beheerd door onafhankelijk netwerkbeheerder Tennet. Het beheer en transport op regionaal niveau is belegd bij een aantal regionale netbeheerders. De netwerkbeheerders bespreken periodiek in het platform integrale veiligheid vraagstukken op het gebied van continuïteit en veiligheid.
- De aardgassector is in toenemende mate geliberaliseerd. Hiertoe is de aardgasinfrastructuur losgekoppeld van de producenten en de leveranciers van aardgas en ondergebracht bij de Gasunie. Gas Transport Services B.V. (GTS) is als dochter van N.V. Nederlandse Gasunie opgericht voor de uitvoering van de transport en beheertaken. Het beheer en transport van de (regionale) distributienetwerken vallen onder verantwoordelijkheid van een tiental regionale netbeheerders.
- De oliesector is vrijwel geheel in handen van private partijen. Deze zijn georganiseerd in brancheorganisaties, waarvan de belangrijkste zijn: de VNPI (oliemaatschappijen), VOTOB (tankopslagbedrijven), NOVE (handelaren), BOVAG en Beta (Tankstation ondernemingen).

Dreigingen:
Hoewel de energievoorziening ingericht is op verschillende eventualiteiten, blijven er dreigingen die de voorzieningszekerheid van energie in gevaar kunnen brengen. Een belangrijke dreiging blijft de afhankelijkheid van het buitenland voor verschillende energiedragers, zoals kolen, olie en in toenemende mate gas en LNG. Bovendien kan bewust menselijk handelen de nodige schade aanrichten aan vitale energie-infrastructuur en kunnen extreme weersomstandigheden leiden tot het uitvallen van elektriciteit, gas of olie infrastructuur. Tot slot is het nuttig om verder te kijken naar de gevolgen van energie-uitval voor andere sectoren. Uit nationaal en internationaal onderzoek blijkt dat er aanzienlijke keteneffecten te verwachten zijn bij het uitvallen van elektriciteit en gas.

Resultaten:
Het wetsvoorstel Informatie uitwisseling ondergrondse netten is inmiddels van kracht geworden en zal naar verwachting leiden tot een daling van het aantal graafincidenten met betrekking tot ondergrondse leidingen en kabels. Met partijen uit de sector olie en gas is, in combinatie met de chemische sector, onderzoek verricht naar de kwetsbaarheid van buisleidingen. Dit onderzoek is verricht door het NAVI. In mei 2008 is het convenant security van de sector olie en de sector (petro)chemie ondertekend door de betrokken ministeries en organisaties. De betreffende bedrijven hebben inmiddels vervolg gegeven

aan dit akkoord om een aantal, door het NAVI, georganiseerde workshops te volgen om een Security Management Systeem in hun organisatie te implementeren. De resultaten en ervaringen uit verschillende oefeningen hebben ertoe geleid dat de sector energie verschillende stappen heeft gezet om zich voor te bereiden op een verstoring. Voorbeelden van oefeningen zijn de oefening met het Alerteringsysteem Terrorisme bestrijding (het ATB van de NCtb), de grote oefening Waterproef en de Emergency Response Exercise 4 van het Internationale Energie Agentschap (IEA). In de eerste beleidsbrief vitaal uit 2005 en de hierop volgende voortgangsrapportages (2006, 2007, 2008) zijn aanvullende maatregelen benoemd ten behoeve van de energie sector. Deze maatregelen zijn grotendeels afgerond, daarnaast wordt gewerkt aan een aantal projecten door het ministerie van Economische Zaken, de sector en anderen. In het kader van de dreigingen uit de Nationale Risico Beoordeling zijn acties ondernomen in de Energiesector om beter voorbereid te zijn om dreigingen zoals de uitbraak van een grieppandemie.

2010 e.v.:

- In opdracht van EZ, in samenwerking met Tennet, wordt er door het NAVI een security onderzoek verricht om te kijken naar de resterende risico's die kunnen leiden tot het uitvallen van het elektriciteitsnetwerk. Uit dit onderzoek kunnen vervolgacties komen die kunnen leiden tot een verbetering van de security van het Elektriciteitsnetwerk.
- In de afgelopen maanden is begonnen met het implementeren van de EPCIP richtlijn. In 2011 zal de implementatie afgrond moeten zijn. Dan moeten de ECI's binnen Europa zijn geïnventariseerd en moet deze infrastructuur voldoen aan de voorwaarden van de richtlijn.
- Er wordt aandacht gegeven aan het vervangen van grijs gietijzeren buisleidingen op kwetsbare plekken in het buisleidingennetwerk. In aanvulling op het security rapport buisleidingen, van het NAVI, wordt een vervolgstudie uitgevoerd om te kijken naar mogelijke vervolgacties.
- De weerbaarheid van alle vitale sectoren tegen verstoringen in de Elektriciteit- respectievelijk de ICT/Telecom sector wordt in kaart gebracht en wordt zo nodig vergroot.
- Er wordt een nationaal responsplan voor Energie opgesteld teneinde een adequate preparatie en respons op incidenten in dit beleidsveld te realiseren.
- In de loop van 2009 is er een akkoord bereikt over een nieuwe EU richtlijn over het aanhouden van strategische voorraden van aardolie en aardolieproducten. Deze nieuwe richtlijn moet op 1 januari 2012- geïmplementeerd zijn in de lidstaten.
- Er wordt gekeken hoe het pakket aan vraagbeperkende maatregelen, teneinde brandstof besparing te realiseren in de transportsector, kan worden vernieuwd.

2 Sector Telecom/ICT

Typering sector:

De Telecommunicatie- en ICT-sector ontwikkelt zich nog steeds in een sneltreinvaart. Deze sector zal steeds verder groeien en deels samengaan met andere sectoren w.o. de audiovisuele sector. Deze convergentie vindt plaats op verschillende niveaus zoals infrastructuur, apparatuur en inhoud. Hierdoor zullen ook verdere veranderingen optreden in productie, distributie en gebruik op zowel nationaal als internationaal niveau. Doordat

criminele activiteiten zich verder blijven verplaatsen naar deze netwerken, vraagt het behoud en verder vergroten van de betrouwbaarheid, beschikbaarheid en veilig gebruik van deze netwerken ook meer aandacht. Voorbeelden van criminele activiteiten zijn het infiltreren in netwerken en ICT toepassingen. Deze activiteiten kunnen negatieve effecten hebben voor de vitale bedrijven en sectoren die gebruik maken van deze ICT-toepassingen en - netwerken.

Netwerk en verantwoordelijkheidsverdeling:
De liberalisering van de telecommunicatiemarkt heeft geleid tot meer en redundante verbindingscapaciteit (verschillende operators voor zowel vaste als mobiele telefonie). Een duidelijke verantwoordelijkheid is bij de aanbieders van telecommunicatiediensten belegd om zorg te dragen voor continuïteit van dienstverlening. Vanwege een commercieel belang zijn deze aanbieders ook zelf in hoge mate gebaat bij een instandhouding van "hun" telecommunicatievoorzieningen. Dit betekent dat ze ook zelf actief maatregelen nemen waar nodig en lopen de belangen van de aanbieders in hoge mate samen met het publieke belang. Bedrijven die internettoegang bieden (o.a. internetproviders) hebben een hoog besef van risico's vanwege de vele dagelijkse aanvallen op het systeem. Partijen hebben onderling veel geregeld om mogelijke schade aan systemen in te dammen. In de vorige Beleidsbrief BVI (16 september 2005) en de sectorrapportages aan de TK (2006, 2007 en 2008) is al aangegeven dat de sector ICT en Telecommunicatie in zijn algemeenheid voldoende maatregelen heeft getroffen, of bezig was te treffen, om de continuïteit van de dienstverlening op adequate wijze te waarborgen. Op basis van opgedane ervaringen is de voorlopige conclusie dat het door het ministerie van EZ en de sector gevoerde veiligheids- en continuïteitsbeleid op orde is.

Dreigingen:
Een aantal bevindingen uit de kwetsbaarheidanalyses is omgezet in maatregelen die onder de beleidsverantwoordelijkheid van het Ministerie van EZ vallen. Het gaat hierbij met name om het verkrijgen van (meer) transparantie in het gebruik van infrastructuren, het verhogen van 'awareness' over een veilig ICT/Telecommunicatie gebruik en het continuïteitsbeleid. Een groot deel van de te nemen maatregelen wordt opgepakt via werkprogramma's van het Agentschap Telecom, het Nationaal Adviescentrum Vitale Infrastructuur, Nationale Infrastructuur ter bestrijding van Cybercrime, en het Programma Digibewust en Digivaardig. Binnen het Nationaal Continuïteitsoverleg Telecommunicatie (NCO-T = voorheen NACOTEL) vindt overleg met de telecomproviders plaats over de implementatie van maatregelen. Daarnaast is een aantal aanbevelingen, welke gericht zijn op een verdere (onderzoekmatige) verdieping met betrekking tot technische- , geografische zaken en verantwoordelijkheden en bevoegdheden, deels meegenomen in het BVI-initiatief gebiedsgerichte benadering en deels als onderdeel van een volgende vitaalcyclus. In de brief van 6 november 2006 aan de Tweede Kamer is via de minister van BZK gemeld dat het ministerie van EZ de voortgang en de primaire beleidsverantwoordelijkheid van enkele vitale elementen heeft overgedragen aan de ministeries van BZK (noodcommunicatiesysteem en maatregelen voor informatievoorziening over calamiteiten) en V&W (radionavigatie voor scheep- en luchtvaart).

Resultaten:

Continuïteit en beschikbaarheid

- De deelnemers van het Nationaal Continuïteitsoverleg Telecomsector (NCOT) hebben tussen 2005 en 2009 deelgenomen aan verschillende workshops om te komen tot intersectorale analyses voor de scenario's grieppandemie en overstroming. In deze workshops is door de deelnemende partijen inzichtelijk gemaakt wat de gevolgen van deze omstandigheden kunnen zijn voor het functioneren van vitale producten en diensten. De onderlinge relaties en afhankelijkheden zijn in kaart gebracht en het sociale netwerk is uitgebreid c.q. verstevigd.
- De Telecomsector is in het derde kwartaal van 2009 aangesloten op het Alertering Terrorismebestrijding (ATb). Het project ICT-verstoring heeft een vervolg gekregen. Een projectorganisatie is ingericht om de weerbaarheid van de vitale sectoren bij mogelijke langdurige uitval van respectievelijk ICT/Telecom en elektriciteit te vergroten.
- Binnen het programma Nationale Veiligheid is het project ICT-verstoring gaande. In samenwerking tussen publieke en private partijen van diverse vitale sectoren, zijn enkele ICT-dreigingscenario's uitgewerkt op basis waarvan risico's en maatregelen zijn bepaald.
- In EU-verband is door zowel publieke als private partijen deelgenomen aan diverse workshops vitale Infrastructuur o.a. binnen European Programme for Critical Infrastucture Protection (EPCIP).

Veilig gebruik

- Binnen het programma Nationale Infrastructuur ter bestrijding van Cybercrime, kortweg NICC, is vooral gewerkt aan het verder uitbouwen van het Informatie Knooppunt Cybercrime (IKC). In 2008 zijn enkele sectoren aangesloten bij Informatieknooppunten w.o. Multinationals – Information Sharing & Analysis Centre (ISAC), de Spoor-ISAC. De Telecomsector sloot begin 2009 aan op het IKC.
- Het onderwerp proces control security (PCS)[4] heeft de afgelopen periode veel aandacht gekregen binnen het BVI project. Op nationaal niveau is binnen het hierboven genoemde IKC een sectoroverstijgend overleg gestart rond PCS. Via het programma NICC zijn tevens twee events georganiseerd die gericht waren op awareness en het uitwisselen van ervaringen. Internationaal is deelgenomen aan het Europese SCADA-platform, European SCADA and Control Systems Information Exchange(EuroSCSIE).
- Op nationaal niveau hebben overheden, het bedrijfsleven en belangenverenigingen samen een Gedragscode Notice-and-Take-Down opgesteld. De NTD-gedragscode schrijft voor hoe particulieren en bedrijven in de online sector omgaan met een melding over onrechtmatige inhoud op het internet.

2010 e.v.:

- Vanuit het NCO-T wordt een blauwdruk ontwikkeld om een risicoanalyse van de hele ICT/Telecom -sector vast te stellen.
- De respons op ICT-incidenten wordt versterkt door ondermeer:

[4] Ook wel SCADA (Supervisory Control And Data Acquisition) genoemd

    - De inrichting in 2010 van een ICT Respons Board , een publiek-privaat samenwerkingsverband waarin deskundigen snel en adequaat kunnen reageren op grote ICT-incidenten.
    - Organiseren van een oefening, aansluitend op de oefening Cyberstorm III van de Amerikaanse overheid.
- De toenemende convergentie van de sector ICT/Telecom en audiovisueel, en de gevolgen hiervan voor de vitale sectoren als gebruiker, wordt opnieuw in kaart gebracht. Indien nodig zal hier een nadere risicoanalyse plaatsvinden.
- Het programma NICC loopt af op 31 december 2009. Het netwerk dat is opgebouwd en is aangesloten op het IKC zal zonder meer voort blijven bestaan.
- NL zet zich in voor internationale samenwerking op het gebied van internetveiligheid, o.a. via EU/ENISA activiteiten. Daartoe zal ondermeer actief worden meegewerkt aan de uitvoering van de resolutie inzake netwerk- en informatiebeveiliging die in december 2009 door de Europese raad is aangenomen.
- Verder wordt in samenwerking met het bedrijfsleven een routeplan opgesteld, dat gericht is op het verbeteren van ICT-security met bijzondere aandacht voor process control systems.

3 Sector Drinkwater

Typering sector:
Drinkwater is voor de mens een primaire levensbehoefte. Drinkwater wordt naast consumptie voor de mens tevens gebruikt voor andere huishoudelijke doeleinden, proceswater, bluswater en consumptiewater voor dieren. De continuïteit en kwaliteit van de levering van drinkwater zijn sinds jaren goed geregeld. De Leveringsplannen van de waterbedrijven zijn hiervoor het beleidskader. Met de nieuwe Drinkwaterwet (zie hierna) wordt het opstellen van leveringsplannen wettelijk geregeld Daarnaast is binnen de sector een basisniveau van beveiliging afgesproken, het zogenoemde GoedHuisVaderschap. De Leveringsplannen en het afgesproken niveau van beveiliging dekken de vitale belangen van de drinkwatervoorziening voldoende af.

Netwerk en verantwoordelijkheidsverdeling:
De verantwoordelijkheidsverdeling bij de openbare drinkwatervoorziening is wettelijk geregeld. Op dit moment nog in de Waterleidingwet en het Waterleidingbesluit. In 2009 is de nieuwe Drinkwaterwet gepubliceerd. Deze wet treedt op 1 januari 2011 in werking, gelijktijdig met het Drinkwaterbesluit, waarvan het ontwerp momenteel in procedure is.
De kern van de verantwoordelijkheidsverdeling is dat de overheid zorg draagt voor de drinkwatervoorziening en de drinkwaterbedrijven belast zijn met de feitelijke uitvoering daarvan (aanleg en beheer van infrastructuur, productie en distributie). Deze uitvoering moet in overeenstemming zijn met de wettelijke eisen ten aanzien van drinkwaterkwaliteit, leveringszekerheid en doelmatigheid. Het rijk heeft hierbij het eerstelijns toezicht. Voor bestuursorganen van de overheid geldt dat de duurzame veiligstelling van de drinkwatervoorziening een dwingende reden van groot openbaar belang is. Wettelijke eisen ten aanzien van leveringszekerheid hebben betrekking op normale en buitengewone omstandigheden. De nieuwe wet regelt ook de nooddrinkwatervoorziening en de noodwatervoorziening, zoals die door drinkwaterbedrijven en gemeenten gezamenlijk moet worden ingericht.

Dreigingen:

Na de aanslagen in 2001 hebben de gezamenlijke drinkwaterbedrijven, Vewin, het ministerie van VROM en de AIVD met het project Beveiliging Nederlandse Watersector (Benewater) in kaart gebracht met welke reële bedreigingen ten aanzien van bewust menselijk handelen drinkwaterbedrijven rekening moeten houden en welke haalbare en proportionele beveiligingsmaatregelen getroffen zijn cq getroffen dienen te worden. Dit heeft een pakket maatregelen opgeleverd dat in de drinkwatersector bekend staat onder de naam GoedHuisVaderschap. Sinds 2003 wordt binnen de sector volgens deze methode een beveiligingsniveau gerealiseerd dat - evenals de maatregelen tegen verstoringen met andere oorzaken - gekenmerkt wordt als reëel, haalbaar, en proportioneel. Daarmee wordt bedoeld dat een drinkwaterbedrijf zich beveiligt tegen realistische opponenten, dat de maatregelen in redelijke verhouding staan tot de dreiging, dat deze financieel en technisch uitvoerbaar zijn en ingepast kunnen worden in de dagelijkse bedrijfsvoering. Het maatregelenpakket is gebaseerd op een risicoanalyse waarin in eerste instantie de belangen die het drinkwaterbedrijf wil beschermen, de dreiging en de huidige risico's en mogelijke beveiligingsmaatregelen (de weerstand) in kaart zijn gebracht. Vervolgens wordt gekeken hoe de bestaande maatregelen verhoogd of verbeterd kunnen worden en tegen welke risico's geen of onvoldoende maatregelen bestaan (de restrisico's). Ten slotte wordt uit de diverse mogelijkheden een selectie van samenhangende maatregelen gekozen die aan de genoemde criteria voldoen.

In het kader van het Alerteringsysteem Terrorismebestrijding (ATb) zijn op landelijk niveau kwetsbare drinkwaterlocaties in kaart gebracht.
Bij de vormgeving van het nieuwe Drinkwaterbesluit is ervoor gekozen om het GoedHuisVaderschap als uitgangspunt te nemen. In het Drinkwaterbesluit, dat op 1 januari 2011 in werking treedt, wordt voor de drinkwaterbedrijven een wettelijke verplichting vastgelegd om een verstoringrisicoanalyse op te stellen. Een verstoringrisicoanalyse omvat het inventariseren en analyseren van de voor het leveringsgebied van een drinkwaterbedrijf bestaande en te verwachten dreigingen voor de openbare drinkwatervoorziening. De verstoringrisicoanalyse vormt de basis voor alle continuïteit- en crisisbeheersingsvoorzieningen van elk drinkwaterbedrijf. Tevens is het de basis voor het leveringsplan. De VROM-Inspectie speelt in dit kader een rol bij de toetsing en handhaving.

In aanvulling op de door de drinkwaterbedrijven geïnventariseerde dreigingen, kan de Minister van VROM, wanneer bijvoorbeeld een Nationale Risicobeoordeling door het Ministerie van Binnenlandse Zaken daar aanleiding toe geeft, nationale dreigingen vaststellen welke dienen te worden opgenomen in de (regionale) verstoringrisicoanalyses van de drinkwaterbedrijven.

Resultaten:

De Nederlandse drinkwatervoorziening kent een lange traditie van veilige en gegarandeerde drinkwaterlevering. De drinkwatersector doet haar werk op basis van gedegen wetgeving waaronder waarborgen voor de kwaliteit en de continuïteit van de levering. Daarnaast wordt er door de rijksoverheid, c.q. de VROM-inspectie, permanent toezicht gehouden op de drinkwaterbedrijven. Met de implementatie van maatregelen die naar voren kwamen uit het project Beveiliging Nederlandse Watersector (Benewater) is er in de drinkwatersector de afgelopen jaren al veel geregeld. De sector heeft flink geïnvesteerd in verbetering van de beveiliging. Binnen de sector is er alles aan gedaan om de risico's die de als realistisch geachte scenario's met zich meebrengen, af te dekken. De

onderstaande resultaten, producten en lopende activiteiten zijn er op gericht om deze traditie voor de Nederlandse burger voort te zetten. Vanaf medio 2003 heeft de sector fors geïnvesteerd om het basisbeveiligingniveau, het zogenoemde GoedHuisVaderschap, die de sector heeft afgesproken te implementeren. Basis voor deze aanpak was het project Beveiliging Nederlandse Watersector (Benewater), dat het volgende in kaart bracht:
met welke reële bedreigingen waterbedrijven rekening moeien houden (basisdreigingsbeeld) en welke haalbare en proportionele beveiligingsmaatregelen getroffen zijn, cq. getroffen kunnen worden.
Op grond van het project Benewater voorziet de sector in een lokale beveiligingsaanpak waarbij een samenhangend pakket van technische, personele, organisatorische en ICT-maatregelen is geïmplementeerd.

Als eerste vitale sector in Nederland zijn de drinkwaterbedrijven aangesloten op het Alertertingssysteem Terrorismebestrijding (ATb) van de Nationaal Coördinator Terrorismebestrijding (NCTb). De drinkwaterbedrijven hebben in dit kader per opschalingsniveau (weerstands)maatregelen geformuleerd die bij een terroristische dreiging in werking worden gesteld.

In de nieuwe drinkwaterregelgeving (zie ook hiervoor) zal het afgesproken niveau van beveiliging en crisisbeheersing juridisch worden vastgelegd. De bedrijven dienen hieraan invulling te geven via het Leveringsplan. De Leveringsplannen en het afgesproken niveau van beveiliging dekken de vitale belangen van de drinkwatervoorziening voldoende af. In het hoofdstuk Leveringszekerheid zijn de kaders gegeven voor leveringszekerheid en continuïteit, oefenfrequentie, en nood(drink)watervoorziening. Het Drinkwaterbesluit, dat deze kaders nader concretiseert, zal op 1 januari 2011 van kracht worden.

Overige activiteiten
De drinkwatersector neemt deel aan de door de NCTb georganiseerde oefeningen in het kader van het Alerteringssysteem Terrorismebestrijding (ATb). Daarnaast is in het afgelopen jaar wederom zowel operationeel als bestuurlijk veel geoefend. Zo zijn er oefeningen gehouden en heeft overleg plaatsgevonden met gemeenten, politie, Veiligheidsregio's, waterbeheerders en provincies. Een groot aantal drinkwaterbedrijven heeft deelgenomen aan de oefening Waterproof. Drinkwaterbedrijven - als zijnde crisispartner van de Veiligheidsregio's - starten momenteel de samenwerking met de Veiligheidsregio's op. In juni 2008 heeft Vewin, namens de sector, een brief aan de voorzitter van het Veiligheidsberaad gestuurd met daarin het voorstel om een eenduidig afsprakenkader tussen alle drinkwaterbedrijven en Veiligheidsregio's op te stellen. Het gaat hierbij om samenwerkingsafspraken inzake de preparatie en respons op drinkwater gerelateerde incidenten. Op hoofdlijnen zijn een negental samenwerkingsafspraken in de brief uiteengezet. Vervolgens zijn twee drinkwaterbedrijven met een Veiligheids- en Politieregio een pilot gestart om deze negental afspraken op regionaal niveau uit te werken en invulling aan te geven. De afspraken worden in een samenwerkingsconvenant vastgelegd. Het gaat hierbij om afspraken op het gebied van melding en alarmering, planvorming, participatie aan regulier overleg, gezamenlijk oefenen, participatie aan crisisteams, coördinatie bij veiligheidsregio-overschrijdende incidenten, informatievoorziening, crisiscommunicatie. C2000 en bewaking en beveiliging van kwetsbare drinkwaterlocaties.

Om een zo breed mogelijk draagvlak voor het convenant te creëren hebben de ministeries van BZK en VROM, VNO-NCW en Vewin als klankbord gefungeerd. Het convenant werd op 29 mei 2009 door bovengenoemde partijen ondertekend, en zou het vertrekpunt kunnen zijn voor een landelijk samenwerkingsconvenant tussen alle drinkwaterbedrijven en Veiligheidsregio's. Daarnaast hebben de drinkwaterbedrijven zich aangesloten bij het Nationaal Informatieknooppunt Cybercrime en vormen daarbinnen een afzonderlijk informatieknooppunt, het zogenaamde Water-ISAC.

Op grond van de rol van het Ministerie van VROM in de responsfase, zijnde onder ander het geven van advies over de levering van drinkwater onder verstoorde omstandigheden, is besloten een zogenaamde Eenheid Planning en Advies drinkwater (EPA-d) op te richten. Het responsplan voor deze EPA-d is gereed en het implementatietraject is gestart. Ten slotte opereren zowel VROM, RIVM, als de sector, in internationale programma's en samenwerkingsverbanden om vernieuwende kennis en inzichten ten aanzien van beveiliging en de preparatie op crisissituaties in de drinkwatersector op te doen.

2010 e.v.:
Implementatie nieuwe regelgeving (Drinkwaterwet en Drinkwaterbesluit).

4 Sector Voedsel

Typering sector:
De sector voedsel bestaat uit primaire productie in Nederland, verwerking, handel, transport en uiteindelijke distributie naar de consument. Het is een complex geheel met vele actoren. Er zijn vele productieketens en er zijn om die reden veel substitutiemogelijkheden. Nederland is grotendeels zelfvoorzienend en neemt een spilfunctie in voor de distributie van voedsel naar diverse buurlanden.

Netwerk en verantwoordelijkheidsverdeling:
Het gehele systeem van voedselvoorziening in Nederland is een zeer omvangrijk en zeer complex netwerk van vele tienduizenden, private bedrijven (zie ook hiervoor). Bovendien is er een grote verwevenheid met het buitenland, zowel EU als ook mondiaal. Nederland is voor de meeste basisvoedselproducten meer dan zelfvoorzienend; Nederland is zelfs één van de grootste voedselexporteurs ter wereld. Dit betekent, dat Nederland over een nationale voedselproductiecapaciteit beschikt, die voor verschillende producten (veel) groter is dan de nationale behoefte.

Voor de voedselvoorziening van de Nederlandse consument zijn vanuit het oogpunt van Nationale Veiligheid (vitale bedrijven) vooral de laatste schakels in de voedselketens van belang. Hierbij moet men denken aan de levensmiddelenindustrie en de retail. Beide kennen een goed georganiseerde koepelorganisatie, zijnde de Federatie Nederlandse LevensmiddelenIndustrie (FNLI) en het Centraal Bureau Levensmiddelen (CBL; de supermarkten). Het ministerie van LNV heeft met enige regelmaat overleg met deze organisaties, waarbij ook de onderwerpen veiligheid, crisis en weerbaarheid aan de orde kunnen komen.

LNV is primair verantwoordelijk voor de totale voedselketen van productie tot verwerking, en samen met EZ verantwoordelijk voor distributie. Conform de inzichten van het

interdepartementale project Bescherming Vitale Infrastructuur (BZK sinds 2002) ligt de verantwoordelijkheid voor de bedrijfscontinuïteit primair bij de eigenaren/beheerders van betreffende organisaties en ondernemingen binnen deze sectoren. De entamerende en/of beleidsondersteunende rol van LNV hiertoe is een taak, die in 'vredestijd' gestalte krijgt (Draaiboek Crisisbeheersing Voedselvoorziening, Ministerie van LNV, 2009).

Dreigingen:
De voedselproductie en –distributie zijn dermate geografisch gespreid over het gehele land en tot op plaatselijk niveau, dat deze daarmee uit het oogpunt van dreigingen een robuust karakter hebben en een grote mate van weerbaarheid laten zien. In geen van de branches zal door het uitvallen van de grootste productielocaties de voedselvoorziening in gevaar komen. Bovendien kunnen veel levensmiddelen in geval van nood vervangen worden door andere; een hoge substitutiegraad. In tijd van crisis zal o.a. het VoedingsCentrum Nederland (VCN) een rol spelen bij de advisering omtrent een gezond voedingspatroon op basis van de beschikbare levensmiddelen.

De kwetsbaarheid van de voedselvoorziening ligt meer in het vlak van de afhankelijkheid van andere vitale producten en diensten, waarvan de belangrijkste zijn drinkwater, energie en (weg-)transport. Deze maken alle deel uit van de Vitale Infrastructuur, zodat ze ook onder het programma Nationale Veiligheid vallen.
De tweede groep begingebeurtenissen, die een belangrijke impact zouden kunnen hebben, bestaat uit bewust menselijk handelen in de vorm van een terroristische aanslag of van sabotage, gericht op het contamineren van voedsel. Wat dat betreft is er een samenhang tussen voedselvoorziening en voedselveiligheid. De Voedsel- en WarenAutortiteit (VWA), vallende onder de ministeries van LNV en VWS, beschikt over een eigen crisisorganisatie en kan in dergelijke gevallen adequaat optreden..

Resultaten:
Afgelopen jaren is door LNV onderzoek uitgevoerd en zijn er gesprekken en workshops met de sector georganiseerd. De conclusie die door de sector gedeeld wordt is dat de mens niet zonder voedsel kan, maar dat de voedselvoorziening in Nederland robuust is. Voor de meeste voedselcomponenten is Nederland zelfvoorzienend. Daarbij heeft Nederland een belangrijke rol in de handel.

Er zijn sectoren waar de sector voedsel afhankelijk van is, in meer of mindere mate. Dit blijkt onder andere uit workshops die gehouden zijn met diverse sectoren. Het betreft dan logistiek/distributie en de energiesector. Op gebied van logistiek zijn echter meerdere modaliteiten waarvan gebruik gemaakt kan worden om voedsel te distribueren. In tijd van crisis zijn er diverse noodwetten waar overheid gebruik kan van maken om controle uit te oefenen over voorraden en distributie. Dit kan alleen in zeer bijzondere gevallen.

De huidige consumptie kenmerkt zich door producten die makkelijk klaar te maken zijn en waar veel bewerking voor heeft plaatsgevonden. Deze processen kosten energie. Echter, de sector geeft aan, dat in geval van een crisis deze voorbehandeling deels overgeslagen kan worden en de consument voorzien kan worden van basisvoedselcomponenten.

2010 e.v.:
Voor de sector voedsel zijn voedselzekerheid en voedselveiligheid elementair. Hiervoor wordt op diverse vlakken beleid ontwikkeld. Er is voor deze twee onderdelen op vele

niveaus aandacht. Van nationaal niveau, tot internationaal via EU en FAO (Food and Agriculture Organization van de VN). De weerbaarheid van de sector zal met zekere regelmaat onderzocht moeten worden. Dit is in lijn met wat afgelopen jaren gebeurd is. Zolang Nederland grotendeels zelfvoorzienend is en in staat is om de voedselveiligheid op een hoog niveau te houden is de sector robuust en weerbaar. Via bestaande organisaties zoals productschappen kan indien nodig overleg gevoerd worden over relevante onderwerpen in het kader van de vitale infrastructuur.

5 Sector Gezondheid

Typering sector:

De gezondheidszorg is maatschappelijk een cruciaal product. De sector kan problemen ondervinden door uitval in andere sectoren, (energie, drinkwater, communicatie, transport) of door bewust menselijk handelen (terreur) en kent dus een belangrijke mate van afhankelijkheid van een aantal andere vitale sectoren. Het uitvallen van de gezondheidszorg heeft niet direct gevolgen op het niveau van "vitaal" voor de overige sectoren. Wel is de dreiging van een grieppandemie in de Nationale Risicobeoordeling (NRB) als grootste risico voor de nationale veiligheid naar voren gekomen. Een grieppandemie kan tot gevolg hebben dat 30 % van de beroepsbevolking uitvalt en heeft daarmee effect op vitale sectoren. De continuïteit van de sector gezondheidszorg speelt een cruciale rol bij een grieppandemie.

Vitale diensten

Drie deelprocessen, te weten spoedeisende medische hulpverlening, essentiële medische producten en sera en vaccins, zijn van groot belang voor de sector.

Spoedeisende medische hulpverlening

De geneeskundige hulpverlening is verdeeld over een groot aantal particuliere ondernemingen en private beroepsbeoefenaars, zoals ziekenhuizen en huisartsen. Door de kwantiteit en spreiding zal uitval van één instelling of enkele beroepsbeoefenaars voldoende opgevangen kunnen worden binnen de sector. Grootschalige uitval van spoedeisende medische hulp en overige ziekenhuiszorg zal in de regel het gevolg zijn van het (deels) uitvallen van een andere vitale sector.

Essentiële medische producten

Langdurige uitval van essentiële medische producten (denk aan insuline) zal leiden tot levensbedreigende situaties of tot ernstig en blijvend letsel onder burgers.

Sera en vaccins

Bij een grootschalige uitbraak van een onbekende infectieziekte zal er in de regel al snel sprake zijn van een crisissituatie. Niet alleen de gezondheidszorg heeft last van (de gevolgen van) bijvoorbeeld een grieppandemie. Door ziekte of de zorg voor zieke naasten kunnen mensen hun rol in het dagelijkse leven niet meer (geheel) vervullen. Dit kan leiden tot ontwrichting van de maatschappij en maatschappelijke onrust. Hier ligt ook de relatie met de inzet van OOV-diensten.

Netwerk en verantwoordelijkheidsverdeling:
De sector kent van oudsher sterke netwerken binnen de gezondheidskolommen. Er zijn beroepsspecifieke netwerken waar het ministerie van VWS bij is aangesloten en waarvan tijdens crisis snel gebruik kan worden gemaakt. Deze netwerken fungeren ook onder normale omstandigheden. Het is afhankelijk van het dreigingstype van welk netwerk gebruik wordt gemaakt. Voor crisissituaties zijn bijstandsafspraken gemaakt. De medische en zorginstellingen zijn zelf primair verantwoordelijk voor de risicobeheersing binnen het eigen bedrijf.

Dreigingen:
Alle dreigingen zijn relevant voor de sector gezondheidszorg zodra de gezondheid van de bevolking daarbij in het geding komt. In de NRB is de grieppandemie als grootste risico voor de nationale veiligheid naar voren gekomen. Zeker gezien de manifestatie van de Nieuwe Influenza A (H1N1) virus is het afgelopen jaar dan ook vooral ingezet op deze dreiging. Ook heeft deze dreiging voor de sector gezondheidszorg de meeste impact op het eigen functioneren en blijkt bij dit dreigingstype de afhankelijkheid van andere vitale sectoren van gezondheidszorg.
De belangrijkste kwetsbaarheid van de sector ligt in de afhankelijkheid van andere sectoren, zoals energie en drinkwater en de beschikbaarheid van voldoende (personeel voor) opvang van veel slachtoffers. Daarnaast is de sector voor de meeste medische producten internationaal afhankelijk. Ook discontinuïteit in het vervoer van deze producten kan de sector raken. De genomen maatregelen van de afgelopen periode hebben zich onder andere op deze kwetsbaarheden gericht.

Resultaten:
- Met de Wet op de Veiligheidsregio's zullen ook de GGD-en en GHOR territoriaal congruent zijn met de veiligheidsregio's. Er wordt gestreefd naar 1 directeur publieke gezondheid, zodat ook de GGD-en nauwer betrokken worden bij de rampen –en crisisbeheersing op regionaal niveau.
- Ziekenhuisrampopvangplannen (Zirop's) en continuïteitsplannen zijn voor 85 % gerealiseerd en verbreed naar de gehele zorgsector, inclusief huisartsen en GHOR.
- Vanaf 2008 is 10 miljoen euro op jaarbasis beschikbaar om de zorgsector op te leiden, te trainen en multidisciplinair te oefenen.
- Er zijn meerdere multidisciplinaire oefentools aangereikt aan de sector, waaronder een internetmodule.
- Er zijn afspraken gemaakt met zorgverzekeraars en de aanbieders van zorg over de continuïteit van de intramurale zorg.
- De ministeries van BZK en VWS hebben het project Griep en Maatschappij gedaan om de maatschappelijke effecten van een grieppandemie op o.a. de vitale sectoren verder in kaart te brengen. Hiervoor is ook met het Strategisch Overleg Vitale Infrastructuur (SOVI) samengewerkt.

2010 e.v.:
- Nu de continuïteitsplannen en integrale zorgplannen voor een groot deel aanwezig zijn in de sector, wordt gestreefd naar intersectorale plannen en op den duur ook bovenregionale plannen. Dit moet leiden tot nog meer afstemming en gezamenlijke voorbereiding binnen de sector. Dit is een hoge mate van planvorming, maar de plannen gaan uit van het principe dat ze gericht zijn op een

structuur om crisis en rampen op te vangen. Ze zijn globaal van karakter en gebaseerd op scenariodenken.
- De aanlevering van het essentiële medische product voor de nucleaire geneeskunde is kwetsbaarder geworden door de uitval van de installatie Petten. Dit is een zorgpunt waar aan gewerkt wordt.

6 Sector Financieel

Typering sector:
In de financiële sector gaan grote bedragen om en vinden grote hoeveelheden transacties plaats. Wanneer de financiële sector geheel of gedeeltelijk uitvalt kunnen de financieel economische gevolgen en het maatschappelijk ongemak, dan wel maatschappelijke onrust bij uitval, al vrij snel zeer hoog oplopen. Daarom wordt de financiële sector tot de vitale sectoren gerekend.

Vitale diensten
De vitale diensten die worden aangeboden door de kerninfrastructuur van de financiële sector betreffen het betalingsverkeer en het effectenverkeer en zijn als volgt onder te verdelen:

Toonbankbetalingsverkeer
Onder het toonbankbetalingsverkeer (contant en elektronisch) vallen chartale betalingen (betalingen met bankbiljetten en munten) en elektronische betalingen met de pinpas (debitcard), creditcard- en chipknipbetalingen. Consumenten vertrouwen op een soepel lopend betalingsverkeer in onder andere winkels, uitgaansgelegenheden en tankstations.

Massaal giraal betalingsverkeer
Tot het massale girale betalingsverkeer ('betalen op afstand') dat door de financiële sector wordt afgewikkeld, behoren crediteurenbetalingen (overschrijvingen, acceptgiro's), incasserende instrumenten (incasso's) en salarisbetalingen (overschrijvingen). Ook het toonbankbetalingsverkeer (via betaalautomaten) en de geldopnamen bij geldautomaten en aan de balie worden in de systemen voor massaal giraal betalingsverkeer verwerkt.

Hoogwaardig betalingsverkeer tussen banken
Hieronder valt het betalingsverkeer tussen banken en andere kapitaal- en geldmarktbetalingen (waaronder treasuryverkeer van grote bedrijven). Voorts valt hieronder de afwikkeling van valutatransacties.

Effectenverkeer
Onder het effectenverkeer valt de handel, de verevening en de afwikkeling van effecten- en derivatentransacties. Voorts valt hieronder de buitenbeurshandel (Over-The-Counterhandel) die zich niet bij particulieren, maar vooral in het wholesale segment afspeelt.

Bij (gedeeltelijke) uitval van het toonbankbetalingsverkeer is sprake van maatschappelijke ontwrichting, omdat betalingen niet kunnen plaatsvinden of vertraging oplopen. Toonbankbetalingen kunnen verricht worden met verschillende betaalmiddelen waardoor

uitval van korte duur van één betaalmiddel kan worden opgevangen door een ander betaalmiddel. Deze opvangmogelijkheden zijn echter beperkt, zowel in tijd als in omvang.

Als de verwerking van het massale betalingsverkeer stilligt, leidt dit niet direct tot maatschappelijke ontwrichting, maar kan dit naarmate de uitval langer duurt tot financieel-economische schade leiden. Ook bij uitval van het hoogwaardige betalingsverkeer tussen banken en het effectenverkeer is maatschappelijke onrust minder waarschijnlijk, maar kan aanzienlijke financieel-economische schade optreden, vanwege de zeer hoge bedragen die daarin omgaan. Uiteindelijk kan bij uitval van het betalingsverkeer ook immateriële schade optreden in de vorm van vermindering of verlies van vertrouwen in (onderdelen van) de financiële sector. Dit laatste kan bovendien economische gevolgen op middellange termijn hebben. Anders dan in bijvoorbeeld de drinkwater- of de elektriciteitssector zijn niet direct mensen- of dierenlevens betrokken bij uitval of verstoring van de financiële sector.

Vitale Knooppunten
De financiële kerninfrastructuur omvat de instellingen die zorgen voor de verwerking van het belangrijkste deel (in omvang en/of waarde) van de vitale diensten. De vitale knooppunten van die instellingen zijn de locaties en systemen van waaruit de processen en diensten negatief beïnvloed kunnen worden.

Netwerk en verantwoordelijkheden:
In de afgelopen jaren is binnen de financiële sector een gedegen netwerk opgezet waarin de continuïteit van deze sector als geheel behandeld kan worden. Hierbij zijn specifieke gremia opgezet om gezamenlijk crisis te kunnen behandelen en beheersen (Escalatiecommissie), om specifiek terroristische dreigingen te kunnen behandelen (Werkgroep Alertering Financiële Sector (WAFS)) en om gezamenlijk strategisch beleidsmatig vraagstukken op het terrein van business continuity en vitale infrastructuur te kunnen behandelen (Platform Business Continuity Vitale Infrastructuur – Financiële Sector (BC VIF)). Op deze gremia wordt later nog ingegaan.
Door de opzet van dit netwerk waarbij ook partijen van buiten de financiële sector, zoals de NCTb en AIVD, nauw betrokken zijn is het mogelijk om als gezamenlijke partijen de verantwoordelijkheid te nemen voor de bescherming van de vitale producten en diensten in de financiële sector.

Op individueel niveau zijn financiële instellingen zelf verantwoordelijk voor het nemen van verschillende technische en organisatorische maatregelen, de uitwijk- en backup maatregelen en business continuityplannen en –strategieën om de continuïteit te waarborgen. De Nederlandsche Bank houdt toezicht op de business continuity van de onder toezicht staande instellingen. Tenslotte is het ministerie van Financiën op nationaal niveau de eerst verantwoordelijke voor de vitale sector Financieel.

Dreigingen:
De vitale infrastructuren waarvan de financiële sector het meest afhankelijk van is, zijn elektriciteit en (tele)communicatiediensten waaronder het internet. De instellingen van de financiële kerninfrastructuur hebben noodvoorzieningen waarmee uitval van elektriciteit gedurende een beperkte periode kan worden opgevangen. Het hoogwaardige betalingsverkeer en het effectenverkeer zullen daarom minder geraakt worden dan het

toonbankbetalingsverkeer en het massaal giraal betalingsverkeer. Uitval van elektriciteit van langere duur kan ook voor de kerninfrastructuur uiteindelijk problemen opleveren.

Van uitval van telecommunicatiediensten kunnen alle vitale financiële diensten veel hinder ondervinden. Hier kan een onderscheid gemaakt worden in algemene telecommunicatiediensten en de meer specifieke diensten. Tot de algemene telecommunicatiediensten behoren de vaste- en mobiele telefoonnetwerken en het internet. Hiervan zijn het toonbankbetalingsverkeer en deels het massaal giraal betaalverkeer afhankelijk. Specifieke diensten zijn de dedicated netwerken, deze worden vooral in het hoogwaardige betalingsverkeer en het effectenverkeer en deels in het massaal giraal betalingsverkeer gebruikt.

Steeds meer infrastructuur van de financiële sector is in het buitenland komen te liggen. Uitval van deze in het buitenland gelegen infrastructuur kan grote gevolgen hebben voor het betalings- en effectenverkeer in Nederland. Deze buitenlandse financiële instellingen vallen onder andere jurisdicties en dit geeft nieuwe afhankelijkheden.

Specifieke dreigingen
Een belangrijke rol bij het identificeren van risico's voor de vitale infrastructuur van de financiële sector is weggelegd voor de nationale risicobeoordeling (NRB). In de risicobeoordeling worden de grootste risico's voor de Nederlandse samenleving geïdentificeerd. Voor elke dreiging is aangegeven hoe groot de kans is dat het beschreven scenario zich voordoet en hoe groot de impact dan zou kunnen zijn.

De NRB identificeert als de grootste dreigingen voor de nationale veiligheid: een verstoring van onze energievoorzieningen (elektriciteit, olie of gas) en ict-voorzieningen (internet, telecommunicatie en dataverkeer), moedwillig handelen en terrorisme, EDO (Ergst Denkbare Overstroming) en een grieppandemie. Elk van deze risico's is in 2005 genoemd bij de dreigingen voor de vitale financiële infrastructuur.

In bovenstaande passage, over de afhankelijkheden van de financiële sector, bleek hoe afhankelijk de financiële sector is van elektriciteit en (tele)communicatiediensten. Een verstoring van de energievoorziening kan leiden tot elektriciteitsuitval, en telecommunicatie-uitval behoort tot een ict-verstoring. Daarmee zijn verstoringen aan energievoorzieningen en ict-voorzieningen dreigingen, die indien deze zich zouden voordoen, een hoge impact kunnen hebben op de financiële vitale infrastructuur. Een uitbraak van een grieppandemie is momenteel gaande. De kans hierop was de afgelopen jaren al sterk toegenomen ten opzichte van 2005. De kans op een grote overstroming wordt net als in 2005 relatief gering beschouwd. Voor beide gebeurtenissen geldt dat ze een grote impact kunnen hebben op de vitale infrastructuur van de financiële sector indien ze zich voordoen.

De afgelopen jaren is er een intensivering van de dreigingen op het terrein van cybercriminaliteit en cyberterrorisme waargenomen. Zo werd Estland in 2007 slachtoffer van een grootschalige cyberaanval. Doelwit van deze aanval waren de websites van belangrijke banken, kranten, televisiestations en overheid. Deze websites waren dagenlang uit de lucht en op straat ontstonden rellen, waarbij één dode en 150 gewonden vielen. De financiële sector is een doelwit van cybercriminaliteit en cyberterrorisme en dergelijke aanvallen kunnen leiden tot openbare ordeverstoringen.

Resultaten:
In de sectorrapportage van 2005 is gemeld dat binnen de financiële sector sprake is van een hoog risicobewustzijn. Er is serieus werk gemaakt van continuïteitsbeleid. Financiële instellingen hebben verschillende technische en organisatorische maatregelen genomen waaronder uitwijk- en backup maatregelen en business continuityplannen en –strategieën om de continuïteit te waarborgen. Op individueel niveau zijn instellingen zelf verantwoordelijk. Van groot belang is dat Business continuity een aandachtspunt is voor De Nederlandsche Bank bij de onder toezicht staande instellingen. Het business-continuitybeleid en -management van de financiële kerninfrastructuur worden periodiek getoetst aan een specifiek voor deze infrastructuur opgesteld normenkader.

Diverse gremia zijn in de afgelopen jaren opgezet om sectorbreed maatregelen te treffen tegen mogelijke dreigingen voor de vitale infrastructuur. Voor het crisismanagement binnen het Nederlandse betalings-en effectenverkeer is ten tijde van de invoering van de euro de 'Escalatie-commissie Betalings- en Effectenverkeer'opgezet. In deze commissie hebben de verschillende instellingen zitting die gezamenlijk de financiële kerninfrastructuur van het betalings- en effectenverkeer in Nederland vormen. De leden van de Escalatiecommissie hebben het mandaat om bij (dreigende) instellingsoverstijgende operationele crises in het betalings- en effectenverkeer de noodzakelijke maatregelen af te spreken.

Daarnaast is een aantal maatregelen genomen om het beschermingsniveau tegen terroristische dreigingen verder te verhogen. Zo is de financiële kerninfrastructuur in mei 2006 via de Werkgroep Alertering Financiële Sector (WAFS) toegetreden tot het Alerteringssysteem Terrorismebestrijding (ATb) van de NCTb. In deze werkgroep zijn verschillende financiële instellingen, De Nederlandsche Bank, de NCTb en het ministerie van Financiën vertegenwoordigd. Doel van de werkgroep is het borgen van het Alerteringssysteem Terrorismebestrijding (ATb) voor de financiële sector.

Een derde initiatief is het Platform Business Continuity Vitale Infrastructuur – Financiële Sector (BC VIF), dat sinds 2009 bestaat. Het platform heeft tot doel om de initiatieven op het vlak van business continuity en bescherming van vitale infrastructuren beter te kunnen coördineren en als financiële sector gezamenlijke standpunten te kunnen innemen. Beleidsmatige onderwerpen op het gebied van business continuity worden hier besproken en het platform is een klankbord voor de vertegenwoordigers van de financiële sector in diverse nationale en internationale gremia. Ook fungeert het platform als aanspreekpunt voor (nieuwe) initiatieven vanuit de overheid.

Deze gremia hebben ervoor gezorgd dat voor de verschillende partijen duidelijk is wat hun verantwoordelijkheid is. Er is inzicht gekomen in elkaars prioriteiten en maatregelen. Ook zijn er vaste aanspreekpunten en processen ingericht. Hiermee is er ook een goed functionerend netwerk gecreëerd. Dit alles is een duidelijke stap voorwaarts ten opzichte van vier jaar geleden.

In 2005 bleek uit de kwetsbaarheidsanalyse een sterke afhankelijkheid van vitale diensten in de elektriciteits- en met name de telecomsector. Om die reden is door het ministerie van Financiën in samenwerking met De Nederlandsche Bank en het ministerie van Economische Zaken eind 2005 een scenariodag georganiseerd. Experts van de drie

sectoren hebben de intersectorale afhankelijkheden nader bestudeerd en besproken. In 2007 zijn de afhankelijkheden van financiële processen van de telecomvoorzieningen met behulp van diverse scenario's verder in kaart gebracht.

Om de bewustwording over ICT-afhankelijkheid te vergroten, heeft de sector financieel in 2007 meegedaan aan de interdepartementale oefening Shift Control. Naast het ministerie van Financiën deed de Escalatiecommise Betalings- en Effectenverkeer mee aan deze oefening. In Shift Control is gekeken naar de besluitvormingsprocessen en informatie-uitwisselingen op ambtelijk en politiek niveau, met als doel het verder professionaliseren van de interdepartementale crisisbeheersing.

In mei 2009 organiseerde De Nederlandsche Bank in samenwerking met de instellingen in de Escalatiecommissie een marktbrede oefening. In deze oefening werden alle diensten en instellingen in de financiële sector geraakt door de gebeurtenissen uit het scenario. Het scenario had met name betrekking op het moedwillig verstoren van het betalingsverkeer door hackers. Naast het oefenen van het nemen van de noodzakelijke maatregelen werd deze oefening vooral gehouden om de verantwoordelijkheidsverdeling en communicatie te oefenen.

In het kader van het ATb hebben er ook verschillende activiteiten plaatsgevonden. In september 2006 heeft de sector deelgenomen aan een workshop over de systematiek van de het alerteringsproces. Vervolgens hebben diverse soorten oefeningen plaatsgevonden: bereikbaarheidstests, in 2007 een zogenaamde table-top oefening en in 2009 een operationele oefening.

De financiële sector besteedt veel aandacht aan business continuity om rampen en crises, zoals een grieppandemie en een ernstige overstroming, zo goed mogelijk te kunnen doorstaan. Voor de grieppandemie is vanuit het ministerie van Binnenlandse Zaken een brief gestuurd naar de financiële instellingen. Deze brief bevat handreikingen voor een instellingsspecifiek continuïteitsplan.

Effectiviteit beschermingsmaatregelen
In de afgelopen jaren is er veel kennis opgedaan over de dreigingen voor de financiële kerninfrastructuur. Er zijn veel preventieve- en repressieve maatregelen genomen om de impact van zulke gebeurtenissen te reduceren. Deze maatregelen hebben geleid tot een hoger beschermingsniveau van de financiële sector. Duidelijk is dat er vanuit de private- en publieke sector een hoog ambitieniveau ligt om het beschermingsniveau van de financiële kerninfrastructuur zo goed mogelijk in te richten.

<u>2010 e.v.</u>
Aandachtspunten
Om het beschermingsniveau verder te verhogen zijn op een aantal aandachtspunten aanvullende maatregelen noodzakelijk. Het eerste aandachtspunt is de samenwerking tussen de financiële sector en de veiligheidsregio's. Deze samenwerking is cruciaal bij de uitval van de financiële kerninfrastructuur omdat het de impact van uitval van financiële kerninfrastructuur kan reduceren. De afgelopen jaren zijn er stappen gezet in de samenwerking, aanvullende maatregelen zullen deze samenwerking verder moeten complementeren.

Een tweede aandachtspunt voor de komende tijd zijn de afhankelijkheden van de financiële sector van andere vitale diensten, met name de elektriciteit- en (tele)communicatiediensten. Deze afhankelijkheid dient nader geanalyseerd te worden om te bepalen of in aanvulling op de maatregelen die zijn getroffen in de afgelopen jaren extra maatregelen genomen dienen te worden om de vitale financiële infrastructuur nog verder voor uitval van elektriciteit en (tele)communicatiediensten te beschermen.

Een derde aandachtspunt is dat steeds meer infrastructuur van de financiële sector in het buitenland is komen te liggen. Uitval van deze in het buitenland gelegen infrastructuur kan grote gevolgen hebben voor de Nederlandse economie en -samenleving. De samenwerking met de partijen in het buitenland die verantwoordelijk zijn voor de vitale infrastructuur, die deels al bestaat, zal verder worden uitgebouwd. Deze samenwerking zal de partijen, die verantwoordelijk zijn voor de Nederlandse financiële infrastructuur, duidelijkheid geven voor de te nemen maatregelen in de eigen business-continuitystrategie en crisismanagement-aanpak.

Samenwerking tussen de diverse betrokken partijen zal er zorg voor dragen dat de aandachtspunten invulling krijgen. Om dit proces op weg te helpen hebben het ministerie van Financiën en De Nederlandsche Bank besloten een werkgroep in te stellen. De werkgroep zal de inventarisatie die in 2004 was gemaakt over de vitale infrastructuur van de financiële sector actualiseren en zich daarbij concentreren op de hierboven omschreven aandachtspunten. De update zal in samenwerking met het Platform Business Continuity Vitale Infrastructuur Financiële sector, de Escalatiecommissie en de Werkgroep Alertering Financiële Sector plaatsvinden.

Conclusie
De financiële sector heeft sinds de vorige sectorrapportage flinke stappen voorwaarts gezet in de bescherming van de financiële kerninfrastructuur. Er is in de financiële sector een gestructureerde verantwoordelijkheidsdeling opgezet en een goed functionerend netwerk gecreëerd. Er zijn maatregelen genomen die regelmatig worden getoetst aan de hand van verschillende scenario's. Ook is er serieus werk gemaakt van het continuïteitsbeleid. Wel blijven er voor de financiële sector enkele punten van aandacht.

7 Sector Keren en beheren oppervlaktewater

Typering sector:
Een belangrijke zorg van de overheid is de bescherming tegen overstroming en de aanwezigheid van schoon en voldoende water voor alle gebruikers. Bescherming tegen overstroming wordt gerealiseerd door het aanleggen/in stand houden van waterkeringen. Er wordt onderscheid gemaakt in vier categorieën:

- primaire keringen: bescherming tegen overstromingen vanuit de grote rivieren, IJsselmeer, Markermeer en de zee;
- regionale waterkeringen: bescherming tegen overstromingen vanuit regionale wateren;
- bemaling: bemalen van het achterland ten behoeve van het beschermen tegen wateroverlast;
- waterkwaliteit: voorkomen van grootschalige vervuiling van oppervlaktewater.

Een object is als vitaal aangemerkt wanneer bij falen een gevolgschade ontstaat groter dan 5 miljard euro of een groot aantal dodelijke slachtoffers zal vallen.

Analyse van de categorieën leidt tot de volgende conclusies:

- Primaire waterkeringen: het merendeel van de primaire keringen (ca 75%) wordt als vitaal aangeduid.
- Regionale waterkeringen: een klein percentage van de regionale keringen (ca 10%) wordt als vitaal aangeduid.
- Gemalen: slechts een klein aantal (maximaal 10) gemalen moet als vitaal worden beschouwd.
- Waterkwaliteit: wordt, gelet op de gehanteerde definities, hier niet als vitaal aangemerkt.

Netwerk en verantwoordelijkheidsverdeling:

De sector keren en beheren oppervlaktewater kenmerkt zich als een voornamelijk publieke sector, met een door partijen sterk gevoelde verantwoordelijkheid in de zorg voor de continuïteit van de dienstverlening. Rijksoverheid, waterschappen, gemeenten en veiligheidsregio's werken gezamenlijk aan de bescherming van de vitale infrastructuur om een geaccepteerd veiligheidsniveau te realiseren.

Dreigingen:

De sector keren is in de eerste plaats gevoelig voor natuurrampen: het hele stelsel van waterkeringen is erop gericht om overstromingen door extreem hoogwater al dan niet gecombineerd met hevige storm te voorkomen. Er is een kleine kans dat een waterkering bezwijkt omdat de belasting hoger is dan waaraan de waterkering volgens de wettelijke eisen moet voldoen. Het bezwijken van waterkeringen door andere oorzaken (al dan niet bewust menselijk handelen) en technische en organisatorische oorzaken mag niet helemaal worden uitgesloten. Met vandalisme worden beheerders regelmatig geconfronteerd. Ook een terroristische aanslag is niet geheel ondenkbaar. Deze zal echter alleen effect hebben in een scenario met een zelden voorkomende hoge waterstand. Vanwege deze noodzakelijke combinatie wordt de waarschijnlijkheid van terroristische verstoring met vitale gevolgen niet hoog geacht. Achterstallig onderhoud, en constructie- en ontwerpfouten zijn mogelijke oorzaken, en hebben in de sector al aandacht gekregen. In de normale bedrijfsvoeringprocessen is kwaliteitsborging ingebouwd. De kans dat technisch falen met vitale gevolgen optreedt wordt klein geacht.

Veel kunstwerken zijn afhankelijk van elektriciteit als energiebron. Bij de belangrijke kunstwerken zijn noodvoorzieningen uitgevoerd in de vorm van noodaggregaten en/of dubbele systemen met verschillende energiebronnen. Veel kunstwerken kunnen ook handmatig worden bediend.

Resultaten:

De Waterwet (voorheen: Wet op de waterkering) is een belangrijk instrument om calamiteiten door overstroming (natuurrampen) te voorkomen. De normering voor de primaire keringen is in deze wet opgenomen. De keringen worden elke zes jaar getoetst op sterkte. Wanneer na toetsing de keringen niet blijken te voldoen worden maatregelen genomen: de keringen worden versterkt of er worden maatregelen genomen die de waterstand verlagen (ruimte voor de rivier). Het beschermingsniveau varieert van 1/250 tot 1/10.000 per jaar.

Omdat het aanpassen van een waterkering pas gebeurt nadat deze in de toetsing onveilig is gebleken zal er altijd een periode bestaan waarin deze niet aan de wettelijke normen voldoet. Deze situatie is inherent aan de systematiek van de Waterwet. Het voorbereiden

en uitvoeren van projecten kost tijd, daarbij moeten ook wettelijke procedures worden doorlopen. Het Rijk vergoedt 100% van de kosten van de versterkingswerken en heeft daarbij te maken met budgettaire beperkingen.
In de periode 1995-2005 is door sterke aandacht op preventie bescheiden voortgang geboekt in de rampenbestrijding, waaronder oefeningen, crisisplannen en samenwerking tussen waterbeheerders en calamiteitenorganisaties. Paraatheid was in die periode vrijwel exclusief het domein van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties, provincies en gemeenten.

In geval van een bijna-overstroming treffen waterbeheerders noodmaatregelen om extra bescherming te bieden, zoals het aanbrengen van zandzakken en schotbalken. Mocht het tot een daadwerkelijke overstroming komen dan wordt de schade beperkt door secundaire dijken die het achterland compartimenten verdelen Een aantal belangrijke compartimenteringdijken wordt voor dit doeleind onderhouden (zgn C-keringen, bijvoorbeeld de Knardijk in Flevoland en de Diefdijk in de Betuwe) maar er zijn ook veel oude in onbruik geraakte dijken die niet met dit oogmerk worden onderhouden.

De overheid heeft bestaande procedures met betrekking tot het aannamebeleid voor wat betreft het screenen van personeel.

2010 e.v.:
De huidige veiligheidsnormen voor primaire waterkeringen zijn afkomstig uit de jaren vijftig van de vorige eeuw. In de tussentijd zijn de bevolkingsdichtheid en de te beschermen economische waarden toegenomen, waarmee het risico (kans x gevolg) op een overstroming is veranderd. Een traject om tot normen te komen die beter aansluiten op de risico's is gestart, met als doel een principebesluit in 2011.
Op grond van een kritische beoordeling van de paraatheid voor een overstromingsramp (RBSO, 2006) heeft het kabinet een Taskforce Management Overstromingen ingesteld. Deze TMO heeft in de periode 2007-2008 een impuls gegeven aan het bewustzijn bij professionals en bestuurders zowel bij waterbeheerders als bij veiligheidsregio's. Belangrijke instrumenten hiervoor waren een subsidieregeling en een meerdaagse overstromingsoefening Waterproef. In de eindrapportage stelt de TMO dat veel voortgang is geboekt maar dat op diverse terreinen aanvullende maatregelen zinvol zijn. Het kabinet heeft in een reactie hierop een aantal van deze aanbevelingen overgenomen, in het bijzonder:

- Het versterken van nationale planvorming en coördinatie;
- Het informeren en stroomlijnen van informatievoorziening;
- Het versterken van de samenwerking binnen de waterkolom en tussen waterkolom en veiligheidsregio's.

Inmiddels is een Stuurgroep Management Overstromingen ingericht waarin waterschappen en Rijkswaterstaat gezamenlijk in de periode t/m 2010 invulling hieraan geven.

8 Sector Openbare Orde en Veiligheid

Typering sector:
De primaire taak van de OOV-sector (brandweer, politie en geneeskundige hulpverlening bij ongevallen en rampen (GHOR) en waar nodig ondersteuning door Defensie) is het handhaven van de openbare orde, het verlenen van hulp in noodsituaties en het zorgdragen voor de veiligheid in Nederland. Grootschalige en langdurige uitval van (delen

van) deze sector kan leiden tot ontwrichting van de Nederlandse samenleving. Omdat alternatieven voor deze diensten die langdurig en op grote schaal inzetbaar zijn, beperkt beschikbaar zijn, wordt de OOV-sector als vitaal beschouwd.

Voor een adequate taakuitoefening is de OOV-sector afhankelijk van een drietal vitale hoofdaspecten:

1. Menskracht (inzet OOV personeel).
2. Materieel (Vaar- voer- en vliegtuigen en werkprocesondersteunende voorzieningen).
3. Communicatie- en informatievoorzieningen (meldkamers, inclusief de in de meldkamers gebruikte informatie- en communicatiesystemen zoals C2000, Geïntegreerd Meldkamer Systeem, alarmnummer 112 en telefonie, Waarschuwings- en Alarmeringssysteem en Openbaar Meld Systeem).

Netwerk en verantwoordelijkheidsverdeling:

De regionale bestuurlijke regie op de brandweerzorg, de GHOR en de rampenbestrijding en crisisbeheersing wordt bij inwerkingtreding van de Wet veiligheidsregio's formeel bij de veiligheidsregio's belegd. Voor de politie ligt die regie bij de regionale colleges in de politieregio's.

Daarnaast is een wijziging van de Politiewet in voorbereiding om de eenheid van de politie te vergroten en het gemeenschappelijk functioneren te verbeteren. Voor wat betreft de veiligheidsregio's zullen de voorzitters formeel bijeenkomen in het Veiligheidsberaad. Ten aanzien van de politie komen onder andere diezelfde voorzitters bijeen in het Korpsbeheerdersberaad, ondersteund door de Raad van korpschefs. Voor zowel de politieregio's als de veiligheidsregio's wordt hiermee een formele gemeenschappelijke afstemming- en besluitvormingstructuur gerealiseerd en beide beraden krijgen een aantal bovenregionale taken toebedeeld.

Vooruitlopend op de inwerkingtreding van de wetten zijn onder andere via convenanten afspraken gemaakt om de inspanningen, om tot een efficiënte en kwalitatief hoogwaardige organisatie van de OOV diensten te komen, extra kracht bij te zetten. Deze ontwikkeling draagt bij aan een vereenvoudigde samenwerking, multidisciplinaire inzet en planmatige regionale en bovenregionale voorbereiding op rampen en crises en verhoogt daarmee de slagvaardigheid en weerbaarheid van de hulpverleningsdiensten.

Zowel het Korpsbeheerdersberaad als het Veiligheidsberaad voeren separaat overleg met de Minister over de landelijke doelstellingen op het gebied van rampenbestrijding en crisisbeheersing. Door de dubbelrol van regionale bestuurders wordt evenwel een multidisciplinair en integraal regionaal veiligheidsbeleid gegarandeerd en kan daadkrachtig worden opgetreden bij een ramp of crisis. De minster van BZK is in dit kader verantwoordelijk voor sturing door middel van de landelijke doelstellingen ten aanzien van de rampenbestrijding en crisisbeheersing en stelt landelijke kwaliteitseisen aan de betrokken organisaties die door de Inspectie Openbare Orde en Veiligheid worden getoetst.

Dreigingen:

De regionalisering beoogt burgers beter te beschermen tegen risico's en een betere hulpverlening en nazorg te bieden bij rampen en crisis. Een robuustere regionale organisatie kan zich immers beter voorbereiden op dreigingen doordat een samenhangend beleid voor alle hulpverleningsdiensten het multidisciplinair oefenen en samenwerken ondersteunt. Door middel van een risicoprofiel worden bovendien de risico's in een bepaalde regio inzichtelijk gemaakt, zodat de benodigde operationele prestaties van de hulpverleningsdiensten kunnen worden geborgd. Om het gevraagde niveau van

hulpverlening te kunnen bieden is het echter ook van belang dat de diensten zelf bestand zijn tegen de dreigingen. Zo zijn er maatregelen genomen om de voortgang van vitale processen te garanderen indien de in de Nationale Risicobeoordeling gesignaleerde risico's voor de Nederlandse samenleving zich zouden voordoen.
Zo speelt bij een Ergst Denkbare Overstroming met name de beperktere beschikbaarheid van werknemers die door de overstroming hun werk niet kunnen bereiken en de beperktere inzetbaarheid van materieel vanwege de onbegaanbaarheid van bepaalde gebieden een rol. Een overstroming kan bovendien tot een elektriciteitsverstoring of daarmee verband houdende ICT uitval leiden. Elektriciteitsverstoring kan invloed hebben op de inzet van materieel, omdat bepaalde apparatuur in uitrukkende voertuigen dient te worden opgeladen. Daarnaast kan elektriciteit- en ICT verstoring de noodzakelijke communicatie ten behoeve van de inzet van hulpverleners ernstig verstoren. In geval van een grieppandemie zal met name het aspect menskracht onder druk komen te staan en daarmee de processen waarbij de inzet van voldoende personeel met de juiste kennis en ervaring essentieel is. Moedwillig handelen kan bovendien met betrekking tot alle drie de vitale hoofdaspecten tot verstoring leiden.

Resultaten:
Onder andere door de regionalisering verder vorm te geven, is de afgelopen jaren veel gedaan om de rampenbestrijding op orde te brengen en de slagvaardigheid en weerbaarheid hulpverleningsdiensten te verbeteren. Dit vraagt om een andere manier van samenwerken en een eenduidig samenhangend beleid om deze multidisciplinaire samenwerking te ondersteunen. Er zijn in dit kader vele maatregelen genomen om tot een heldere verantwoordelijkheidsverdeling te komen, capaciteiten te versterken en inzicht in elkaars capaciteiten te verbeteren en om de ontwikkelingen te borgen. Hierover is regelmatig aan de kamer gerapporteerd. Het ging daarbij onder andere om:

- Intensivering Civiel-Militaire Samenwerking: in de ontwikkeling van Defensie als vangnet tot een structurele veiligheidspartner zijn sinds 2005 veel stappen genomen, onder andere door de bestuursafspraken in 2007 en de daarop opgestelde catalogus gegarandeerde militaire capaciteiten. Daarnaast is het gezamenlijk oefenen en opleiden geïntensiveerd.
- Oefenen: Om de ontwikkelingen ten behoeve van het op orde brengen van de rampenbestrijding in te bedden in de verschillende organisaties, speelt het samenhangend beleid ten behoeve van het opleiden, trainen en oefenen een belangrijke rol. De nationale oefening Waterproef in november 2008 is een van de voorbeelden van een grootschalige oefening met een multidisciplinair karakter.
- Informatiemanagement: Een van de prioriteiten die in het kader van de basisvereisten aan de veiligheidsregio's is gesteld is de invoering van het netcentrisch werken in de regio's, zodat bestuurders en operationele diensten vrijwel gelijktijdig over een eenduidig beeld van een ramp of crisis kunnen beschikken.
- Continuïteit eigen vitale processen:Er bestaan veel maatregelen om de weerbaarheid van de hulpverleningsdiensten te vergroten onder andere door noodstroom en alternatieve communicatiemiddelen. Wanneer deze maatregelen evenwel niet voldoende zouden blijken, kan veelal worden gesteund op inzet vanuit andere regio's of vanuit Defensie via het Landelijk Operationeel Coördinatie Centrum (LOCC). Daarnaast heeft de continuïteit bij griep het afgelopen jaar ook bij de OOV diensten extra aandacht gekregen.

2010 e.v.:
Alhoewel de OOV sector als geheel een bepaalde kwaliteit en veerkracht kent die de bescherming van de samenleving waarborgt, dienen de verschillende organisaties in deze ontwikkelingen ook continu oog te houden voor de vraag of de doorgang van hun eigen specifieke vitale diensten kunnen worden gewaarborgd. Dit vraagt om extra aandacht voor continuïteitsmanagement vanuit een ander perspectief dan de gemaakte kwaliteitsslag waarin multidisciplinaire samenwerking centraal staat. Onder andere ter voorbereiding op de griep hebben de organisaties daar al veel stappen in ondernomen. Daarnaast lopen er een aantal projecten waarbij de eigen continuïteit wederom onder loep zal worden genomen, zoals:

- Weerbaarheid en respons bij uitval elektriciteit en ICT: Momenteel wordt er gewerkt aan extra maatregelen die de weerbaarheid en respons versterken bij uitval of verstoring van elektriciteit en ICT. In 2010 zal dit traject ook de OOV-sector bestrijken.
- Robuustheid crisiscommunicatiemiddelen*:*Op basis van onderzoek naar de afhankelijkheden van crisiscommunicatiemiddelen zullen dit jaar aanvullende maatregelen worden gekozen ter verbetering van de robuustheid.

9 Sector Rechtsorde

Typering sector
De sector rechtsorde beslaat de verantwoordelijkheid voor het adequaat functioneren van de strafrechtsketen. Binnen de strafrechtsketen worden drie vitale organisaties / onderdelen onderscheiden:

- Het Openbaar Ministerie;
- De Rechtspraak en
- De Dienst Justitiële Inrichtingen.

Hoewel er sprake is van drie specifieke vitale organisaties / onderdelen, neemt dit niet weg dat de andere organisaties / onderdelen binnen de strafrechtsketen de eigen continuïteit en voorbereiding op mogelijke crises structureel geagendeerd hebben.

Openbaar Ministerie
De vitale belangen van het OM zijn:

- het proces van strafvervolging en rechtspraak (rechtshandhaving);
- de informatie die daarvoor benodigd is (ICT);
- de (keten) partners waarmee een afhankelijkheidsrelatie bestaat;
- het personeel.

De Rechtspraak
De vitale belangen van de rechtspraak zijn, naast de rechterlijke macht:

- andere organisaties / onderdelen binnen de strafrechtsketen, te weten het Openbaar Ministerie en de Dienst Justitiële Inrichtingen;
- afhankelijkheidsrelaties van derden, zoals de advocatuur maar ook gerechtsdeurwaarders, tolken en andere partijen die de rechtspraak ondersteunen.

Dienst Justitiële Inrichtingen

Het kernproduct van DJI is detentie. Een deel van de gedetineerden vormt een gevaar voor onze samenleving en kan grote problemen veroorzaken wanneer hun detentie als gevolg van een crisissituatie (tijdelijk) niet kan worden geëffectueerd.

Netwerk en verantwoordelijkheidsverdeling

De minister van Justitie is onder meer verantwoordelijk voor strafrechtelijke rechtshandhaving en terrorismebestrijding. Bij veel rampen of crisis speelt strafrechtelijke rechtshandhaving een rol.

De drie genoemde organisaties / onderdelen binnen de strafrechtsketen kennen elk een grote mate van autonomie maar zijn tegelijkertijd sterk afhankelijk van elkaar. Het ministerie van Justitie heeft op het gebied van continuïteit en crisisbeheersing vooral een coördinerende en adviserende rol. De departementale crisisorganisatie is met name ingericht op het ontsluiten van informatie uit de diverse onderdelen en (taak)organisaties binnen de sector rechtsorde.

Tijdens de voorbereidingen op de grieppandemie is gebleken dat een snel en adequaat beeld van de stand van zaken in alle departementale onderdelen en (taak)organisaties binnen de strafrechtsketen en dat de bestaande ketenafhankelijkheden helder zijn.

Dreigingen en kwetsbaarheden

Voor de sector rechtsorde zijn de volgende vijf dreigingen uit de Nationale Risicobeoordeling relevant:

- Grieppandemie;
- EDO (ergst denkbare overstroming);
- verstoring van de voorziening van elektra, gas en water;
- verstoring van ICT-voorziening;
- moedwillig menselijk handelen (terrorisme, cybercrime).

Resultaten

De organisaties / onderdelen binnen de strafrechtsketen hebben zich middels continuïteit-, crisis- en calamiteitenplannen en de daarin opgenomen maatregelen op genoemde dreigingen en kwetsbaarheden voorbereid. De maatregelen in de continuiteits-, crisis- en calamiteitenplannen zijn van preventieve, repressieve en correctieve aard.

2010 e.v.:

Een betere voorbereiding op toekomstige crises blijft continu een aandachtspunt. Alleen wanneer de onderdelen / organisaties in de sector rechtsorde toegesneden en voorbereid blijven op toekomstige dreigingen, kan het minimale weerbaarheidsniveau worden gewaarborgd. De dreigingen zijn in toenemende mate complex, grootschalig en intersectoraal en vragen daarmee om heldere snelle besluitvorming en slagkracht. Op het ministerie van Justitie wordt voor de sector rechtsorde dan ook aansluiting gezocht bij de rijksbrede verdere professionalisering in het kader van de nieuwe crisisstructuur op rijksniveau opdat de sector rechtsorde "state of the art" blijft.

10 Sector Openbaar bestuur

Typering sector:
Het openbaar bestuur vervult een bijzondere positie in het project Bescherming Vitale Infrastructuur. Bij grootschalige calamiteiten heeft de overheid - het openbaar bestuur - de integrale zorg voor de openbare orde en veiligheid. De effecten van een verstoring in een willekeurige vitale sector raken daarmee per definitie aan de verantwoordelijkheid van het openbaar bestuur.

Vitaal Openbaar Bestuur richt zich op 2 aspecten:

1. het beschermen van de continuïteit van besluitvorming tijdens de respons op en herstel na uitval van vitale infrastructuur en
2. het beschermen van de communicatiemiddelen voor de noodzakelijke informatie-uitwisseling tijdens (de dreiging van) ernstige calamiteiten tussen overheden en voor communicatie naar de bevolking

Netwerk en verantwoordelijkheidsverdeling:
Als coördinerend Ministerie is Binnenlandse Zaken en Koninkrijksrelaties verantwoordelijk voor de inrichting, werking, samenhang en integrale aanpak van het crisisbeheersingsbeleid (preparatie, respons, herstel) en bijbehorende stelsel. Ieder ministerie is daarnaast zelf verantwoordelijk voor de te nemen crisisbeheersingsmaatregelen op het eigen beleidsterrein en het stellen van kaders voor de maatregelen die vitale bedrijven moeten nemen voor de beheersing van crises.

Bij een lokale of regionale crisis valt de crisisbeheersing onder de verantwoordelijkheid van lokale overheden als de gemeente of veiligheidsregio. Naar gelang de aard en omvang van een incident kan er sprake zijn van opschaling. In samenwerking met de departementale crisiscentra wordt in dat geval de besluitvorming tijdens crises ondersteund door het Nationaal CrisisCentrum (NCC). Het NCC vervult de functie van interdepartementaal facilitair communicatiecentrum en knooppunt van en voor de bestuurlijke informatievoorziening. De operationele inzet en bijstand tijdens grootschalige incidenten wordt door het Landelijk Operationeel Coördinatiecentrum (LOCC) gecoördineerd. Daarnaast wordt de rol van Defensie als structurele partner voor nationale veiligheid steeds verder vorm gegeven.

Het netwerk dat betrokken is bij het waarborgen van de veiligheid van de Nederlandse samenleving is aldus groot en daarom is een eenduidige coördinatie- en besluitvormingsstructuur essentieel. Daarnaast is het ook belangrijk dat bedrijven en burgers hun eigen verantwoordelijkheid kunnen nemen.

Dreigingen:
De Strategie Nationale Veiligheid en Nationale Risicobeoordeling (NRB) die daar onderdeel van vormt, maken het mogelijk om beter in kaart te brengen welke dreigingen er op Nederland af komen en te beoordelen wat er aan capaciteiten versterkt moet worden. Dreigingen zijn in de loop der jaren veranderd en complexer geworden, bijvoorbeeld als gevolg van onderlinge afhankelijkheden. Dit vraagt om een veerkrachtige crisisbeheersing die in kan spelen op die veranderingen. Op basis van de in de NRB gesignaleerde risico's zijn capaciteiten geïdentificeerd waarin geïnvesteerd zal moeten worden om de impact van die risico's het hoofd te kunnen bieden. Het gaat daarbij zowel om specifieke als generieke capaciteiten. De generieke capaciteiten richten zich veelal op de rol die het openbaar

bestuur vervult in het in breder zin verminderen van de impact van dreigingen. In de voortgangsbrief nationale veiligheid wordt bijvoorbeeld expliciet aandacht besteed aan hoe capaciteiten op het gebied van de risico- en crisiscommunicatie kunnen worden versterkt gezien de belangrijke rol die dit speelt in het handelen van de bevolking voorafgaande aan of tijdens crisis. Daarnaast kunnen dreigingen als overstroming, grieppandemie en moedwillig handelen ook een grote impact hebben op de continuïteit van de besluitvorming tijdens crisis zelf. Deze dreigingen, maar ook met name de risico's van uitval of verstoring van elektriciteit en ICT voorzieningen, kunnen eveneens de onderlinge informatie-uitwisseling of communicatie naar de bevolking verstoren. Daarom wordt er voortdurend geïnvesteerd in het verbeteren van de besluitvorming, informatie en communicatie, zodat slagvaardig kan blijven worden opgetreden tijdens crisissituaties en er indien nodig alternatieven voorhanden zijn.

Resultaten:

Vanaf het vaststellen van het beleidsplan crisisbeheersing 2004-2007 en de in mei 2007 vastgestelde Strategie voor Nationale veiligheid zijn veel maatregelen getroffen om de organisatie en effectiviteit van de rampenbestrijding en crisisbeheersing te verbeteren. Hierover is periodiek gerapporteerd aan de kamer. Er is veel geïnvesteerd in een nationale crisisorganisatie waarin het openbaar bestuur een eenduidige rol vervult en zichtbaar optreedt. Hierbij is niet alleen aandacht voor de continuïteit van de besluitvorming, maar ook voor het waarborgen van de kwaliteit van de organisatie en effectiviteit van de crisisbeheersing, zodat kwetsbaarheden in dit proces worden verminderd. Het verhelderen en aanscherpen van verantwoordelijkheden is daar een belangrijk onderdeel van. Ook aan snelle informatievoorziening en crisiscommunicatie is gewerkt gezien het belang voor de kwaliteit van de crisisbesluitvorming en crisisbeheersing. De beleidsdoorlichting crisisbeheersing 2004-2007 onderschrijft dat er veel vooruitgang is geboekt op deze punten. Een aantal voorbeelden van de activiteiten waarover aan de kamer gerapporteerd is, zijn:

- Kwaliteit en beschikbaarheid faciliteiten:Ten behoeve van haar functie als interdepartementaal facilitair communicatiecentrum en knooppunt van en voor bestuurlijke informatievoorziening het NCC in 2006 ingrijpend verbouwd, zodat deze voldoende uitgerust is om aan de informatiebehoefte te voldoen en om de informatie-uitwisseling optimaal te faciliteren. Daarbij had het verminderen van kwetsbaarheden (o.a.door beveiligingsmaatregelen) en de beschikbaarheid van alternatieven (bijvoorbeeld uitwijklocaties en noodstroom) eveneens de aandacht.
- Robuuste communicatiemiddelen: Inmiddels is het contract voor een nieuwe NoodCommunicatieVoorziening (NCV) getekend. Het NCV zorgt ervoor dat bij verstoringen van de openbare voorzieningen toch nog communicatie mogelijk is tussen overheidsorganisaties onderling en met het vitale bedrijfsleven. Juist omdat het een "last resort" communicatievoorziening is, wordt er net als bij het eerdere Noodnet veel aandacht besteed aan de betrouwbaarheid en weerbaarheid tegen fysieke en niet fysieke dreigingen. Voor de communicatie richting de burger wordt daarnaast onder andere ten behoeve van de burgeralarmering gewerkt aan de invoering van Cellbroadcast, de verzending van tekstberichten naar mobiele telefoons via radiogolven.
- Oefenen: Ten behoeve van het behoud en de ontwikkeling van het kwaliteitsniveau en het weerstandsvermogen in de crisisbeheersing, wordt voor de voorbereiding op de crisisbeheersing en het inzichtelijk maken van kwetsbaarheden regelmatig geoefend. Naast een nationale oefening waarbij de

crisisbesluitvorming centraal staat, wordt ook tweejaarlijks een grootschalige multidisciplinaire oefening georganiseerd.

2010 e.v.:
Een betere voorbereiding op toekomstige crises blijft continu een aandachtspunt. Alleen wanneer de crisisorganisatie toegesneden en voorbereid blijft op toekomstige dreigingen, kan immers een bepaald beschermingsniveau worden gewaarborgd. Deze dreigingen zijn in toenemende mate complex, grootschalig en intersectoraal en vragen daarmee om heldere snelle besluitvorming en een vergrootte slagkracht. De verantwoordelijkheid wordt echter niet alleen bij de overheid neergelegd, ook van bedrijven en burgers kan worden verwacht dat ze zich voorbereiden op crises. Deze partijen worden daarin daarom ook in de komende jaren gestimuleerd en ondersteund. Een aantal acties die zullen worden ondernomen zijn:

- Continueren verbetering rijksbrede crisisstructuur: Om de samenwerking van professionals te verbeteren en optimaal te benutten, wordt de komende jaren wederom geïnvesteerd in een hoogwaardige crisisbeheersing op rijksniveau.
- Verbeterde samenwerking met bedrijfsleven: Er is de afgelopen jaren veel geïnvesteerd in publiek-private samenwerking, omdat de rol van het bedrijfsleven bij crisisbeheersing als steeds belangrijker wordt gezien. Zo is onder andere afgesproken dat de samenwerking in de toekomst wordt geïntensiveerd en dat VNO-NCW, als intermediair voor het bedrijfsleven, beter worden meegenomen in de crisisinformatiestroom en meer betrokken worden bij crisisoverleggen.
- Zelfredzaamheid: Met het project zelfredzaamheid zijn concrete acties in gang gezet om de zelfredzaamheid van burgers te stimuleren en te ondersteunen; deze worden voortgezet en uitgebreid.

11 Sector Transport

Typering sector:
Transport is een noodzakelijke voorwaarde voor de economie: personen reizen van en naar locaties waar economische activiteiten plaatsvinden. Toelevering van grondstoffen en distributie van producten vormen de bloedsomloop van de samenleving. Langdurige uitval van (belangrijke elementen binnen) de transportfunctie zou leiden tot grootschalige economische verstoring en daarmee tot maatschappelijke ontwrichting.
In het algemeen is transport niet als kwetsbaar te beschouwen. Het bestaan van dichte netwerken en verschillende modaliteiten naast elkaar maakt verstoring van de functionaliteit als geheel moeilijk voorstelbaar. Bij verstoring van enkele schakels in de netwerken zal de hinder in eerste instantie groot zijn; voor specifieke transportstromen voor vitale functies zullen echter snel alternatieven voor handen zijn.
Een viertal specifieke elementen uit het transportsysteem vraagt echter bijzondere aandacht in het kader van Bescherming van Vitale Infrastructuur. Dit zijn de beide Mainports Schiphol en Rotterdam, specifieke objecten in het Hoofdwegennet en het Hoofdvaarwegennet en tenslotte objecten in het Spoorsysteem[5].

[5] "Binnen de sector transport heeft het spoor als deelsector een plaats gekregen onder andere vanwege de gebleken kwetsbaarheid van het spoor na de aanslagen van 11 maart 2004 in Madrid. Nadere analyses van VenW en de spoorsector hebben geleid de volgende bevindingen:

- uit het oogpunt van de transportfunctie wordt het spoorsysteem niet als vitale infrastructuur beschouwd. Uitval van het spoorsysteem leidt niet tot economische of maatschappelijke

Netwerk en verantwoordelijkheidsverdeling:
De transportsector kenmerkt zich als een voornamelijk geprivatiseerde sector, met een door partijen sterk gevoelde verantwoordelijkheid in de zorg voor continuïteit van de dienstverlening. Een aantal knooppunten in de transportsector is in rijksbeheer. Verkeer en Waterstaat zorgt dat de fysieke basis, het fundament van Nederland, solide is en dat wij ons vlot kunnen verplaatsen, zodat wij hier veilig kunnen leven en werken. Verkeer en Waterstaat draagt daarmee bij aan een dynamische en duurzame samenleving.

Dreigingen:
Een belangrijke rol bij het identificeren van risico's voor de vitale infrastructuur van de transportsector is weggelegd voor de nationale risicobeoordeling (NRB). In de risicobeoordeling worden de grootste risico's voor de Nederlandse samenleving geïdentificeerd. Voor elke dreiging is aangegeven hoe groot de kans is dat het beschreven scenario zich voordoet en hoe groot de impact dan zou kunnen zijn.

De NRB identificeert als de grootste dreigingen voor de nationale veiligheid: een verstoring van onze energievoorzieningen (elektriciteit, olie of gas) en ict-voorzieningen (internet, telecommunicatie en dataverkeer), moedwillig handelen en terrorisme, EDO (Ergst Denkbare Overstroming) en een grieppandemie.
De NRB is voor de transportsector een waardevol instrument gebleken om de robuustheid van de sector op dreigingen te toetsen.

Daarnaast verdient het te vermelden dat per vitaal element in de sector transport unieke kwetsbaarheidsanalyses zijn gemaakt. Zo is bij de kwetsbaarheidanalyse voor de Mainport Rotterdam de nadruk gelegd op verstoring ten gevolge van bewust menselijk handelen. Daarbij is zoveel mogelijk aansluiting gezocht bij de recente en nu nog lopende ontwikkelingen op het gebied van de bescherming van zeevaart, havens en transportketens bij VN en EU . Voor de objecten in het hoofdwegennet/hoofdvaarwegennet is conform de DHM methode per vitaal object een dreigingsanalyse gemaakt. Apart hiervan is voor alle vitale objecten de terroristische dreiging ingeschat. Deze analyse is door Ernst & Young gemaakt en door de AIVD getoetst.

Een van de risicoscenario's bij spoor is een grootschalig uitval van personeel, bijvoorbeeld door pandemie of een staking. Binnen de spoorsector zijn inmiddels scenario's en draaiboeken ontwikkeld in geval van een pandemie.

Het realisme van een pandemie is in de tweede helft van 2009 duidelijk geworden. De kans hierop was de afgelopen jaren al sterk toegenomen ten opzichte van 2005. De kans op een grote overstroming wordt net als in 2005 relatief gering beschouwd. Voor beide gebeurtenissen geldt dat ze een grote impact kunnen hebben op de vitale infrastructuur van de transportsector. Bedrijven in de sector transport besteden veel aandacht aan business continuity om rampen en crises, zoals een grieppandemie, zo goed mogelijk te kunnen doorstaan.

---

ontwrichting op nationale schaal, uitval van de vervoersfunctie leidt niet tot veel slachtoffers, en als de ontwrichting lange tijd duurt zijn er alternatieven voorhanden;

- een aantal objecten is vitaal omdat het verzamelplaatsen zijn van grote aantallen mensen en daarom de potentie heeft van grote aantallen slachtoffers (soft targets)".

Resultaten:
In het algemeen geldt dat VenW als veiligheidsvisie hanteert:

- Veiligheidsniveau door en binnen het ministerie permanent verbeteren (ook wel gedefinieerd als een risiconiveau dat zo laag als mogelijk is: ALARA);
- Veiligheidsniveau expliciet en transparant afwegen;
- Voorbereid zijn op restrisico's;
- Met een werkend veiligheidsmanagement en in een veiligheidscultuur waarbij men aanspreekbaar is op de resultaten en verantwoording kan en wil afleggen.

Dit vindt ook zijn weerslag in de maatregelen die genomen worden ter bescherming van de vitale infrastructuur.

Mainport Schiphol
In 2006 is een Plan van Aanpak Vitaal Schiphol vastgesteld na overleg met stakeholders. Op grond van het Plan van Aanpak is vervolgens een projectorganisatie opgezet met een projectgroep en vijf werkgroepen, die ieder een deelonderzoek uitvoeren. Het voorzitterschap van de projectgroep is geleverd door het Ministerie van Verkeer en Waterstaat. De vijf deelonderzoeken betreffen de thema's vitale objecten (1), buizen en leidingen (2), waterkeren en beheren (3), afhandeling gevaarlijke stoffen (4) en ontsluiting via de weg (5). De taak van de werkgroepen is geweest om een globale risico analyse per vakgebied of object op te leveren, een pakket van mogelijke maatregelen en een kostenschatting. De resultaten van de werkgroepen zijn ingebracht in de projectgroep en met betrokken partijen besproken. Indien aan de orde zullen de uitkomsten verder worden uitgewerkt en geïmplementeerd. De projectgroep komt periodiek bijeen om het project en de voortgang hiervan te blijven monitoren.
Doel van het project Schiphol Vitaal is een inventarisatie van alle vitale onderdelen op de Luchthaven Schiphol die noodzakelijk zijn om de bedrijfsvoering van het luchtvaartbedrijf doorgang te laten vinden. Ook de locatie van functies in Amstelveen (KLM) en Riekerpolder (LvNL) vallen in principe hieronder.
In 2008 is een aanvullend onderzoek gedaan naar de relatie tussen Schiphol Vitaal en de spoorwegterminal/spoortunnel onder Schiphol Plaza. De Schipholspoortunnel bevindt zich voor een groot deel onder het luchthaventerrein. Midden in de tunnel is een treinstation gelegen dat via roltrappen en rolbanen in directe verbinding staat met Schiphol Plaza. Indien opportuun worden de uitkomsten van dit onderzoek met betrokken partijen verder uitgewerkt en zonodig geïmplementeerd.

Mainport Rotterdam
De hele haven beschikt thans over een beveiligingsplan, een Port Security Plan zoals vereist door de Europese Richtlijn Havenbeveiliging. Een integraal onderdeel van dit plan is de lijst met gecategoriseerde objecten aan de hand van de mogelijke gevolgen bij uitval.
In het door de EU vereiste Port Security Plan worden de hoofdlijnen van de organisatie, de taken, bevoegdheden, verantwoordelijkheden en maatregelen in het kader van havenbeveiliging uiteen gezet. Geen enkele autoriteit of organisatie kan eigenstandig de gehele "security" organisatie op zich nemen. Evenals het geval is bij de organisatie van "safety" in het haven- en industriegebied is ook bij security multidisciplinaire samenwerking en eenheid van opvatting van essentieel belang. Een cruciaal uitgangspunt hierbij is dat de rollen en taken ten aanzien van beveiliging zoveel mogelijk aansluiten op de dagelijkse praktijk en werkzaamheden van de betrokken organisaties en bedrijven. Bij inbreuken op de security (bijvoorbeeld aanslagen) kan immers ook de fysieke veiligheid

(safety) direct in het geding zijn. Daarom is ervoor gekozen de reeds bestaande multidisciplinaire samenwerking op het gebied van safety te verbinden aan de multidisciplinaire samenwerking op het gebied van security. Bovendien zijn zowel ten aanzien van safety als security veelal dezelfde organisaties betrokken.
Er zijn maatregelen op verschillende niveau's te onderscheiden:

- organisatorisch
- havenbreed
- per individueel object

Een aanzienlijk deel van de bedrijven in het havengebied voldoet aan de International Ship en Port Facility Security Code. Daarmee heeft men een goedgekeurd beveiligingsplan met opschalingsmogelijkheid volgens drie beveiligingsniveau's: 1, 2 en 3. De autoriteiten in de regio hebben een Plan bij Terroristische Dreiging ontwikkeld waarin afspraken zijn gemaakt over opschaling in geval van een terroristische dreiging.
De verschillende regionale systemen van opschaling waren reeds aan elkaar gekoppeld en zijn onlangs verbonden aan de alerteringsniveau's van het Nationaal Alerteringssyteem. Ook is Rotterdam aangesloten bij het alerteringssysteem voor zeehavens.

Hoofdwegennet en het Hoofdvaarwegennet
Voor de objecten in het hoofdvaarwegen en hoofdwegennet zijn sinds 2005 zijn basismaatregelen getroffen voor toegangsbeheer; de objecten zijn aangesloten op het ATb; het stilstand protocol in tunnels is afgekondigd; informatiebeveiliging heeft plaatsgevonden, zo is gevoelige informatie over de werking en bediening van de vitale objecten van internet verwijderd; een beveiligingsonderzoek heeft voor de vitale objecten plaatsgevonden conform DHM voor Security Management.

Spoorsysteem
Ten behoeve van het borgen van het aspect security op het spoor is die visie vastgelegd in een (concept) kadernota Security Spoor. Doel van deze kadernota is aan de spoorsector een richtinggevend kader te bieden voor het beheersen van de security-risico's van het spoor. Een onderdeel hiervan is het verduidelijken van de rollen, de verantwoordelijkheden en de bevoegdheden van de betrokkenen bij security op het spoor. In het najaar wordt de sectorreactie op deze nota ontvangen. Op basis daarvan zal het ministerie van VenW een standpunt bepalen in de definitieve versie.

<u>2010 e.v.:</u>
Om het beschermingsniveau verder te verhogen verdienen een aantal punten de komende jaren bijzondere aandacht:

- Het eerste aandachtspunt is het –verder- bestendigen van de samenwerking tussen sectorpartijen met de betreffende veiligheidsregio's
- Het tweede aandachtspunt is het verder uitwerken van de afhankelijkheden tussen de transportsector en andere diensten. Het is hierbij noodzakelijk dat de vragende (vitale) partij concretiseert welke behoefte er is in kwalitatieve en kwantitatieve zin onder de heersende omstandigheden, en tracht die behoefte met de betrokken partijen af te dekken.
- Het derde aandachtspunt is dat de samenhang wordt gezien tussen verschillende (inter-) nationale initiatieven op het gebied van bescherming van Vitale Infrastructuur. In dit verband is met name de Europese richtlijn EPCIP van belang.

Voor eind 2010 moeten de lidstaten in kaart hebben gebracht welke vitale belangen in de transport (en ICT) sector van Europees belang zijn en welke beschermende maatregelen daarvoor genomen zijn. Beoordeeld wordt thans of de Rotterdamse haven, Schiphol of het luchtruim als Europees vitaal zijn aan te merken. Als dit het geval is zal dit naar verwachting niet tot extra verplichtingen leiden aangezien de beveiliging van deze infrastructuur in Europees verband al sterk is gereguleerd.

12 Sector Chemische en nucleaire industrie

Typering sector:
De sector bestaat uit de productie, opslag, transport en handel van gevaarlijke stoffen. Door doelbewuste verstoring van deze elementen kan de maatschappij ontwricht worden. Door deze verstoring kunnen bijvoorbeeld gifwolken of radioactieve besmetting ontstaan waardoor overal in het land vele slachtoffers kunnen vallen en gebieden tijdelijk onbewoonbaar zijn. De sector chemie bestaat uit een groot aantal bedrijven die o.a. onder de SEVESO richtlijnen van de EU vallen. Uitgangspunt om iets als een vitaal object/proces aan te merken is het feit, dat er mogelijk meer dan 10 doden buiten de poort kunnen vallen. De sector nucleair bestaat uit zes installaties met de daarbij behorende transporten die vallen onder de Kernenergiewet en onder andere het (in 2005 gewijzigde) verdrag inzake de fysieke beveiliging van kernmateriaal en kerninstallaties.

Netwerk en verantwoordelijkheidsverdeling:
Overheid en bedrijfsleven hebben voor de sector chemie afspraken gemaakt en in de vorm van convenanten vastgelegd. Bedrijfsleven ziet het belang van bescherming. De betrokken partijen vanuit de bedrijven bestaan grotendeels uit de brancheverteGenwoordiging. Het gaat daarbij om onder meer de Vereniging Nederlandse Chemische Industrie (VNCI), de Mineralen en Meststoffen Federatie (MMF), de Vereniging van Kunstmestproducenten (VKP), de Nederlandse Aerosol Vereniging (NAV), MKB Nederland, de Raad Nederlandse Detailhandel, de Vereniging Nederlandse Petroleum Industrie (VNPI) en het Verbond van Handelaren in Chemische Producten (VHCP). De bedrijven zijn zelf verantwoordelijk voor de keuze en het treffen van beveiligingsmaatregelen.
Het verdrag fysieke beveiliging maakt de Staat verantwoordelijkheid voor de regelgeving t.a.v. de beveiliging van kernmateriaal en nucleaire inrichtingen, het toezicht hierop en het inschatten van de dreiging waartegen vergunninghouders zich moeten beveiligen. De vergunninghouders zijn hoofdverantwoordelijke voor de uitvoering van de fysieke beveiligingsmaatregelen. De beveiligingsmaatregelen moeten goedgekeurd worden door de Minister van VROM.

Dreigingen:
Door moedwillige verstoring van de productie, opslag en transport van gevaarlijke stoffen of van grootschalige toepassingen kan de maatschappij ontwricht worden. Door deze verstoring kunnen bijvoorbeeld gifwolken ontstaan waardoor vele slachtoffers kunnen vallen en stadsdelen tijdelijk onbewoonbaar raken. Daarnaast kunnen kwaadwillenden chemicaliën kopen of bepaalde soorten kunstmest en hiermee explosieven maken.

Resultaten:
Met de koepelorganisaties in de chemische- en petrochemische industrie is een convenant afgesloten waarin is vastgelegd dat desbetreffende doelgroep (i.c. BRZO-bedrijven die bij een ernstige calamiteit meer dan tien doden ' buiten de poort' kunnen veroorzaken) een aantal beveiligingsmaatregelen zullen nemen. Op dit moment neemt ruim veertig van de doelgroep van zestig bedrijven deel aan het convenant.

Met de koepelorganisaties uit de kunstmest sector is eveneens een convenant afgesloten betreffende beveiligingsmaatregelen. Uit recent onderzoek blijkt dat het overgrote deel van de locaties, waar deze soorten kunstmest worden geproduceerd, opgeslagen en verhandeld, in een centraal register is opgenomen. De verwachting is dat deze locaties binnen afzienbare tijd een minimumniveau aan beveiligingsmaatregelen zullen hebben getroffen. De VROM-Inspectie zal de mate en wijze van implementatie van deze securitymaatregelen monitoren.
Er is een centraal meldpunt opgericht waar bedrijven en particulieren verdachte transacties in bepaalde soorten kunstmest en chemicaliën, waarmee explosieven gemaakt kunnen worden, kunnen doorgeven. Evaluatie van de opzet en werking van dit meldpunt wordt in het tweede kwartaal van 2010 doorgevoerd.
Ook heeft VROM afspraken gemaakt met de sector (met name de groot- en tussenhandel en de retail) betreffende de verkoop van bepaalde chemische producten aan bijvoorbeeld particulieren. Het gaat hier onder meer om de verkoop van specifieke volumes en percentages van desbetreffende chemische stoffen.

Een analyse naar de bijzonderheden op het vlak van security voor buisleidingen is beschikbaar gekomen. Met de buisleidingensector zal nagegaan worden of, en zo ja hoe, specifieke initiatieven genomen moeten worden om het beveiligingsniveau voor de buisleidingen tot een acceptabel niveau aan te passen.

Bij kunstijsbanen met ammoniakkoeling worden de beveiligingsmaatregelen verder geïntensiveerd. Bij nieuwe kunstijsbanen zal ammoniak uitsluitend in de primaire koelinstallatie worden toegepast en wordt onder de ijsvloer en nabij publieksruimten met andere koudedragers gewerkt. Hierdoor zullen er geen specifieke beveiligingsrisico's voor deze kunstijsbanen aanwezig zijn.

De IAEA heeft op uitnodiging van de Nederlandse overheid de nucleaire installaties beoordeeld op beveiliging. De adviezen hebben voor kerncentrale Borssele geleid tot een aangepast beveiligingsplan. O.a. wordt een weg omgelegd om het observatiegebied te vergroten. Ook de overige installaties zijn bezig met implementatie van de adviezen.

Voor de sector nucleair is in samenwerking met betrokken overheidspartijen (o.a. AIVD en NCTb) en de sector zelf een nationale referentiedreiging opgesteld. Een referentiedreiging (Design Basis Threat) beschrijft de karakteristieken (bijv. type kwaadwillende(n) en hun middelen) van de reëel voorstelbare dreiging tegen de sector of installatie. Dit biedt de basis waarop vergunninghouders hun inrichting en kernmateriaal dienen te beschermen.

Ter implementatie van het gewijzigde verdrag Fysieke beveiliging is de Kernenergiewet gewijzigd en is er een concept Ministeriële Regeling inzake de beveiliging van nucleaire installaties opgesteld. Deze verplicht vergunninghouders om begin 2011 in het bezit te zijn van een door de Minister van VROM goedgekeurd beveiligingspakket. Alle vergunninghouders beschikken nu reeds over een beveiligingspakket op basis van de eisen

die gesteld zijn in de vergunning. Momenteel vind een actualisatieslag plaatst om de IAEA aanbevelingen te implementeren en af te stemmen op de referentiedreiging.

2010 e.v.:

- Het stimuleren van het opzetten en implementeren van het onderdeel beveiliging in het Responsible Care programma bij de chemische industrie.
- Stringentere monitoring van de wijze en mate van implementatie van de convenanten met de kunstmestsector en de olie- en (petro)chemische sector.
- Het versterken van het draagvlak bij de hele doelgroep van bedrijven voor de convenantafspraken.
- Het actualiseren en goedkeuren van de beveiligingspakketten van de vergunninghouders van nucleaire installaties.
- Afspraken maken over de afstemming tussen de interne beveiligingsorganisatie van de installaties en de externe beveiligingsorganisatie door de overheid.
- Afspraken maken ten aanzien van een structurele overheidsinzet bij de beveiliging van het transport van de zwaarste categorie nucleair materiaal ("Categorie I materiaal")