Veranderingen in beleidsprioriteiten bij het Directoraat-Generaal Goederenvervoer (DGG)

Een onderzoek hoe het implementatietraject van het securitybeleid binnen het maritieme cluster van DGG plaats vindt na de gebeurtenissen van 11 september 2001

Werner van Dinter

Delfgauw, september 2004

Veranderingen in beleidsprioriteiten bij DGG

Een onderzoek hoe het implementatietraject van het securitybeleid binnen het maritieme cluster van DGG plaats vindt na de gebeurtenissen van 11 september 2001

Erasmus Universiteit Rotterdam
Faculteit der Sociale Wetenschappen
Vakgroep Bestuurskunde

Afstudeerbegeleider
Dr. H.J.M. Fenger

Doctoraalscriptie
W.R.F. van Dinter (262625)

Voorwoord

Tijdens mijn stageperiode bij het Directoraat-Generaal Personenvervoer (DGP) heb ik kennis gemaakt met het ministerie van Verkeer & Waterstaat (V&W). Na deze stageperiode, het afstuderen aan de opleiding Bestuurskunde aan de Hogeschool ‘s-Hertogenbosch en een korte tussenstap bij KPMG keerde ik terug naar V&W en kreeg een aanstelling bij Rijkswaterstaat. Tijdens die periode schreef ik mij in voor de avondopleiding Bestuurskunde aan de Erasmus Universiteit te Rotterdam. Het studeren beviel mij prima. De sfeer was goed en de medestudenten waren gemotiveerd, juist omdat zij hun studie naast hun baan moesten voltooien.
In mijn tweede studiejaar werd ik beleidsondersteunend medewerker bij de afdeling zeescheepvaart (TZ) van DGG. Tijdens mijn werk op die afdeling vonden de gebeurtenissen in de VS plaats en kon ik van dichtbij waarnemen wat de consequenties daarvan waren voor het DGG-beleid, in het bijzonder voor het zeescheepvaartbeleid.
Ondertussen leerde ik op het werk Hanneke van Steenbergen kennen. Sinds 7 juli 2004 ben ik getrouwd met deze lieve dame en ze heet nu Hanneke van Dinter - van Steenbergen. Hanneke heeft me als geen ander vaak gemotiveerd om mijn studie met goed gevolg af te ronden. Ik dank Hanneke voor haar geweldige steun en stimulans.
Dankzij mijn werk bij DGG heb ik veel in de beleidskeuken van DGG kunnen kijken en de resultaten daarvan kunnen verwerken in het voorliggende onderzoek. Ik wil hierbij de respondenten en de mensen binnen DGG die ik in dit kader van dit onderzoek heb benaderd hartelijk danken. In het bijzonder dank ik Reinoud Pijpers die diverse concepten van dit onderzoek kritisch heeft doorgenomen.
Tot slot dank ik mijn afstudeerbegeleider Menno Fenger voor zijn opbouwende kritiek waaruit telkens bleek dat hij niet alleen uitermate serieus mijn concepten had gelezen en geanalyseerd, maar tevens deze concepten goed kon plaatsen in de wereld van de bestuurskunde.

Werner van Dinter
Delfgauw, september 2004

Samenvatting

In het eerste hoofdstuk worden de probleemstelling, de doelstelling en de redenen voor keuze van dit onderzoek uiteengezet.

De doelstelling van dit onderzoek was als volgt:

> "Het onderzoeken van de ervaringen van zowel interne als externe actoren met de ontwikkeling en de implementatie van het securitybeleid binnen het maritieme cluster van DGG. Dit beleid is een direct gevolg van de gebeurtenissen van 11 september 2001 in de VS."

De centrale vraagstelling luidde als volgt:

> "Hoe vindt de ontwikkeling en de implementatie van het securitybeleid binnen het maritieme cluster van DGG plaats na de gebeurtenissen van 11 september 2001 in de VS?"

In hoofdstuk 2 van dit onderzoek (theoretisch kader) wordt het stappenplan van Price (2004: 331) voor "port security" als kader aangewend voor zowel de theorie als - later in hoofdstuk 4 - de praktijk. In dit stappenplan wordt een aantal stappen onderscheiden: preventie/risico's, detectie, crisismanagement en herstel. Min of meer voorafgaand aan dit stappenplan worden de theorieën van een aantal sociologen behandeld die als het ware het kader vormen voor zowel Price als andere bestuurskundige theorieën. De theorieën van de sociologen Beck, Garland en Perrow plaatsen de kans op een terroristische gebeurtenis in een bredere maatschappelijke context, die gekenmerkt wordt door hoog technologische interactieve relaties. De theorieën van Rosenthal omtrent besluitvorming en de vier risico situaties van Douglas & Wildawsky worden eveneens in dit hoofdstuk behandeld.

In hoofdstuk 3 staat het securitybeleid op papier beschreven. Er wordt ingegaan op het fenomeen terrorisme en de relatie met het securitybeleid binnen het maritieme cluster van DGG. Op 1 december 2002 heeft de Directeur-Generaal (DG) van DGG besloten de Taskforce Security in te stellen. Deze Taskforce moet zorg dragen voor de voorbereiding en uitvoering, in nationaal en internationaal verband, van het V&W security beleid ten aanzien van het goederenvervoer. De Taskforce Security is DGG-breed opgezet. Primair richt deze Taskforce zich op de security van het maritieme cluster. Het maritieme cluster omvat zeescheepvaart en havens. Daarnaast wordt een beschrijving gegeven van de relevante interne en externe actoren en hun rol bij het securitybeleid van DGG.

In hoofdstuk 4 staan de empirische bevindingen centraal. De belangrijkste elementen uit dit hoofdstuk zijn dat er met betrekking tot het dreiginggevaar een eenduidig generiek beeld ontstaat van "er is een dreiging", maar vervolgens schetsen de respondenten uiteenlopende dreigingen.
Ten aanzien van de maatregelen wordt het internationale kader veelvuldig genoemd, met als zeer opmerkelijk element dat de VS met economische sancties achter de hand een dominante factor vormt. De politieke en economische noodzaak zorgt er voor dat de sector goed heeft meegewerkt en nog meewerkt. Zowel impliciet als expliciet is duidelijk dat er een goed ontwikkeld "awareness" niveau aanwezig is. Een aantal respondenten geeft aan dat met het wegvallen van eventuele sancties het in stand houden van de "awareness" wellicht problematisch wordt.
Er zijn geen specifieke opmerkingen gemaakt over de coördinatie en communicatie, anders dan wat betreft het specifieke MKB-kenmerk van een deel van de sector. Deze bedrijven zijn in absolute zin te gering van omvang om de securityproblematiek integraal te betrekken bij de bedrijfsvoering. Bovendien is er bij het MKB weinig aandacht voor het securitybeleid als zodanig, behalve daar waar het gaat om verplichte maatregelen zoals de invoering van de ISPS-code.

In hoofdstuk 5 wordt geconcludeerd dat de in het theoretisch hoofdstuk geschetste complexiteit door de respondenten niet als zodanig wordt ervaren. Met betrekking tot de indeling van Perrow en Douglas & Wildawsky leveren de antwoorden een aanzienlijk eenvoudiger beeld op. Geen complexe hoog

technologische omgeving die als het ware onlosmakelijk de verbintenis moet krijgen met (terroristische) rampen, maar een eenvoudig beeld dat het kan gebeuren. Dit geldt met de nodige veranderingen ook voor de behandelde theorieën van Rosenthal.
Uit de antwoorden van de respondenten zijn geen kritische geluiden opgetekend daar waar het gaat om een gebrek aan communicatie en coördinatie. Gesteld mag worden dat hierover een positief beeld bestaat en dat de respondenten niet spreken over een complexe materie. Vanuit dat oogpunt ontstaat er een beeld van een overzichtelijk opererende overheid.
Er kan niet anders geconcludeerd worden dat DGG haar zaken goed op orde heeft. Juist de coördinatie en informatievoorziening - in feite de kerntaak - wordt positief beoordeeld. De interne maatregelen die zijn genomen met het opschalen van het "traditionele crisisbeleid" naar een steviger en meer politiek orgaan leiden er toe dat adequaat maatregelen worden voorbereid en uitgevoerd. Vastgesteld lijkt te kunnen worden dat deze positieve conclusie mede kan worden getrokken omdat de "awareness" ten tijde van dit onderzoek hoog was. De vraag is echter of deze vaststelling in de toekomst hetzelfde zal zijn.

Op grond van dit onderzoek kan een aantal aanbevelingen gedaan worden voor organisaties die in het securitybeleid binnen het maritieme cluster van DGG een toonaangevende rol hebben:

- De respondenten die het hele securitygebeuren ervaren als "te ver doorgeslagen" en als "een tijdelijke paniekreactie van de Amerikanen, die over een paar jaar wel weer is overgewaaid" zouden wellicht positiever hebben gereageerd als de betrokken partijen meer duidelijkheid hadden gekregen over wat er van hen werd verwacht. Betrokken partijen zouden dan zeer waarschijnlijk de te nemen maatregelen met een meer gedragen gevoel implementeren. Zowel de IMO, de EU en de nationale overheid (hier: DGG) hadden er wellicht beter aan gedaan de betrokken partijen – al ruim voor 1 juli 2004 - goed te informeren over het nut en de noodzaak van het implementeren van de securitymaatregelen;
- Voor de toekomst zal een redelijk goed functionerend informatienetwerk voor het securitybeleid van DGG moeten worden behouden omdat daarmee ook in een situatie die minder dreigend is, effectief beleid kan worden gevoerd. Tevens zullen - analoog aan het onderhouden van "awareness" - op het terrein van crisis en rampenbestrijding in het stappenplan van Price, stappen 1 en 2 onderhouden moeten worden in geval van een dreiging van een terroristische gebeurtenis. Ook indien er geen sprake is van een terroristische gebeurtenis dient op dezelfde manier met de "awareness" ten aanzien van terrorisme gehandeld te worden. Tijdens stap 3 is het onderscheid tussen terrorisme en een andere maatschappelijke dreiging op het terrein van veiligheid niet meer van belang en het verdient aanbeveling dat de betrokken actoren zich hiervan bewust zijn en blijven. Een centraal aansturend orgaan – het meest voor de hand liggend is het NCC – zou met de betrokken actoren in het securitynetwerk kunnen overleggen op welke wijze zij "awareness" geagendeerd houden. Voorts dient te worden onderzocht of er methoden zijn die als "best practise" kunnen worden gehanteerd. De keuze van "best practise" kan vervolgens worden verbreed naar andere organisaties;
- Het politieke gewicht van de nieuwe securitymaatregelen dreigt een aanslag te vormen op de noodzakelijk geachte reductie van de administratieve lasten. Vanuit V&W zal niet alleen handhaving en naleving van de ISPS-code een politiek belangrijk element moeten zijn, maar zal tevens moeten worden gelet op de bruikbaarheid voor de individuele ondernemers van de nieuw te implementeren maatregelen. Voorkomen moet worden dat nieuwe regels leiden tot een grotere administratieve lastendruk.

.

Afkortingen

A	Directie Algemeen Beleid (DGG-onderdeel)
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
AIZ	Afdeling Algemene Internationale Zaken (DGG-onderdeel)
AZ	Ministerie van Algemene Zaken
BNP	Bruto Nationaal Product
BUZA	Ministerie van Buitenlandse Zaken
BVD	Binnenlandse VeiligheidsDienst
BZK	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
CEMT	Conference Européenne des Ministres des Transports
DCC	Departementaal Coördinatie Centrum
DES/VA	Directie Economische Samenwerking/Verkeersafdeling
DG	Directeur-Generaal
DGG	Directoraat-Generaal Goederenvervoer
DGP	Directoraat-Generaal Personenvervoer
DOT	Department of Transportation
DT	DirectieTeam
EMSSA	European Maritime Safety and Security Authority
ETA	Euskadi Ta Askatasuna
EU	Europese Unie
EVO	Eigen Vervoers Organisatie
EVRM	Europees Verdrag van de Rechten van de Mens
GHR	Gemeentelijk Havenbedrijf Rotterdam
GM	Gevolmachtigde Minister
HBR	Haven Bedrijf Rotterdam
HCC	Havencoördinatiecentrum
HDJZ	Hoofddirectie Juridische Zaken
IAPH	International Association of Ports and Harbors
IBT	Interdepartementaal Beleids Team
ICS	International Chamber of Shipping
IHI	Afdeling Infrastructuur, Havens en Intermodaal vervoer (DGG-onderdeel)
ILO	International Labour Organisation
IMO	International Maritime Organisation
IRA	Irish Republican Army
ISM	International Safety Management
ISPS-code	International Ship and Portfacility Security Code
IVW	Inspectie van V&W
IVW/DS	Inspectie van V&W/Divisie Scheepvaart
KFD	KernFysische Dienst
KVNR	Koninklijke Vereniging van Nederlandse Reders
MARPOL	Maritime Pollution
MARSEC	Maritime Security Level
MID	Militaire Inlichtingendienst
MIT	Meerjarenprogramma Infrastructuur en Transport
MIVD	Militaire Inlichtingen- en Veiligheidsdienst
MKB	Midden en Klein Bedrijf
NAVO	Noord-Atlantische Verdragsorganisatie
NBS	Nucleaire Beveiliging Scheepvaart
NCBZH	Nationale Commissie Beveiliging Zeescheepvaart en Havens
NCC	Nationaal Coördinatie Centrum
NDL	Nederland Distributie Land
NHR	Nationale Haven Raad

NSO	Nationale Sigint Organisatie
OESO	Organisatie voor Economische Samenwerking en Ontwikkeling
SB	Schepenbesluit
Sigint	Signal-intelligence
SOLAS	Safety Of Lifes At Sea
SW	Schepenwet
TI	Directie Transport en Infrastructuur (DGG-onderdeel)
TZ	Afdeling zeescheepvaart (DGG-onderdeel)
V	Directie Transportveiligheid (DGG-onderdeel)
VL	Afdeling lading en risicobeleid (DGG-onderdeel)
VM	Afdeling vervoermiddelen (DGG-onderdeel)
VROM	Ministerie van Volkshuisvesting Ruimtelijke Ordening en Milieu
VV	Afdeling verkeersmanagement (DGG-onderdeel)
V&W	Ministerie van Verkeer & Waterstaat
WIV	Wet op de Inlichtingen- en Veiligheidsdiensten
WTC	World Trade Center

Inhoudsopgave

1 Inleiding en probleemstelling

1.1 Inleiding

Op 11 september 2001 troffen drie vliegtuigen strategische doelen in New York en Washington. Een vierde stortte neer in Pennsylvania. De wereld was geschokt en betuigde zijn medeleven met de slachtoffers en zijn afschuw over deze terreurdaad.

In september 2001 werd de angst in de VS nog verder opgevoerd door brieven met wit poeder die onder meer naar het Amerikaanse Pentagon werden gestuurd. Het witte poeder – zo bleek later – bevatte miltvuur (anthrax). De vrees voor grootschalige bio-terroristische aanslagen steeg, maar werd uiteindelijk niet bewaarheid.

De resten van de Twin Towers zijn inmiddels opgeruimd. Op 30 mei 2002 werd “Ground Zero” officieel “schoon” verklaard en er is nog niet precies besloten wat er met “Ground Zero” moet gebeuren. De gevolgen van de aanslagen in de VS, waarbij ruim 3000 doden vielen, zijn echter nog in vele geledingen van de maatschappij zichtbaar. Zowel immaterieel, in de discussies over de multiculturele samenleving, als materieel, in de problemen van met name luchtvaartmaatschappijen zullen de gevolgen van de aanslagen op 11 september 2001 nog lang doorwerken.

Als gevolg van de aanslagen in de Verenigde Staten van 11 september 2001, staat security hoog op de nationale en internationale agenda. Ook Nederland ontkwam niet aan agendering van security op de politieke agenda, zeker voor wat betreft goederenvervoer. Vrij snel na 11 september 2001 werd er een projectteam gestart binnen V&W. Diverse DGG-medewerkers verspreid over de directies zijn vanaf dat moment actief met dit onderwerp bezig. Op 4 november 2002 besprak het Directie Team (DT) een concept plan van aanpak “Maritieme Security” en concludeerde dat het gezien de prioriteit van het onderwerp wenselijk is over te gaan tot versterking, opschaling en verbreding van de structuur van verantwoordelijkheden.

Omdat er in Nederland – tot op heden – nog geen ramp of aanval heeft plaatsgevonden, wordt er niet gesproken over crisisbeleid, maar over securitybeleid. Er dient een duidelijk onderscheid te worden gemaakt tussen de begrippen *“security”* en *“crisis”*. Het security-beleid zoals dit binnen DGG wordt gemaakt heeft als belangrijkste kenmerk dat dit beleid wordt uitgevoerd *vóórdat* een ramp of aanval plaats vindt, en heeft voornamelijk een preventief karakter. Het crisisbeleid daarentegen heeft als belangrijkste kenmerk dat dit beleid wordt uitgevoerd *tijdens en nadat* een ramp of aanval heeft plaatsgevonden (= suppressie).

Het Nederlandse woord “veiligheid” wordt vaak abusievelijk vertaald met “security”. Het begrip veiligheid bestaat uit twee componenten en dat zijn de begrippen “safety” en “security”. Safety omvat alle maatregelen die je treft om het risico van schade door ongelukken te voorkomen en is voornamelijk gericht op maatschappelijke veiligheid, inclusief het milieu. Calamiteiten, zoals ongelukken met een chloortrein, hebben in de preventieve sfeer dus niets te maken met security. Echter, indien een dergelijke calamiteit zich voordoet als gevolg een terroristische actie, zijn de gevolgen identiek met die van een “normale” calamiteit. De suppressie zal in beide scenario’s hetzelfde zijn.
Security omvat alle maatregelen die uitvoerende partijen moeten treffen. Dit kunnen fysieke, organisatorische, beleidsmatige of procedurele maatregelen zijn, om schade of het risico daarop door opzet te voorkomen[1].

[1] De internationale term hiervoor is “unlawful act”.

1.2 Probleemstelling

De probleemstelling valt uiteen in een doelstelling en vraagstellingen:

Doelstelling
Het onderzoeken van de ervaringen van zowel interne als externe actoren met de ontwikkeling en de implementatie van het securitybeleid binnen het maritieme cluster[2] van DGG. Dit beleid is een direct gevolg van de gebeurtenissen van 11 september 2001 in de VS.

Gedurende de periode waarop dit onderzoek betrekking heeft, is de implementatie van het securitybeleid binnen het maritieme cluster van DGG op te vatten als een proces dat nog steeds in een ontwikkelingsstadium verkeert, waarbij tal van actoren een actieve rol spelen. Dit complexe geheel kenmerkt zich door organisatorische, inhoudelijke en procedurele maatregelen, die in dit onderzoek nader uitgewerkt zullen worden.

Centrale vraagstelling
Hoe vindt de ontwikkeling en de implementatie van het securitybeleid binnen het maritieme cluster van DGG plaats na de gebeurtenissen van 11 september 2001?

Vanuit deze centrale vraagstelling kunnen de volgende deelvragen worden afgeleid:
1. Hoe ziet het securitybeleid van het maritieme cluster van DGG eruit en hoe is dit beleid georganiseerd?
2. Welke externe actoren zijn betrokken bij het securitybeleid van DGG?
3. Wat zijn conform het securitybeleid de taken en rollen van de interne en externe actoren?
4. Welke taken en rollen vervullen de interne en externe actoren nu werkelijk?
5. Hoe ervaren de externe actoren het securitybeleid van DGG?
6. Is er sprake van een informatie-uitwisselingsysteem tussen de partijen? Hoe is dit vormgegeven en zijn er mogelijkheden om partijen met elkaar in contact te laten komen en op welke manier kan dit worden vormgegeven?

1.3 Redenen voor keuze van dit onderzoek

Het securitybeleid binnen het maritieme cluster van DGG is een onderwerp dat zich uitstekend leent om nader onderzocht te worden en wel om de volgende redenen:

1. Securitybeleid binnen het maritieme cluster van DGG is een compleet nieuw beleidsterrein.
Mondiaal gezien zijn sommige landen vertrouwd met het begrip security. Zo hebben de Verenigde Staten al langere tijd van doen met terroristische aanslagen, is het “Irish Republican Army (IRA)” in het Verenigd Koninkrijk actief, evenals de organisatie “Euskadi Ta Askatasuna (ETA)[3]” in Spanje. Echter, met name in de Noord-Europese landen zijn terrorisme - en in het verlengde daarvan, de preventie ervan - nieuw te noemen verschijnselen.

Een ministerie als V&W had tot voor 11 september 2001 niet te maken met openbare orde en veiligheid in relatie tot aanslagen als die van 11 september. Wél heeft V&W te maken met veiligheid rondom het goederenvervoer. Alhoewel V&W in principe geen directe bevoegdheden heeft wat betreft veiligheid in relatie tot aanslagen, wordt het beleidsterrein van dit ministerie met terrorisme en security geconfronteerd (bijvoorbeeld: de nieuwe “International Maritime Organisation (IMO)-regelgeving”[4]), maar ook de kwetsbaarheid van de Nederlandse infrastructuur die in principe in beheer is bij Rijkswaterstaat. Andere voorbeelden zijn waterbeheer en waterkering, luchtvaart, binnenvaart,

[2] Het maritieme cluster is te definiëren als een in onderlinge samenhang verzameling van veertien maritieme sectoren, waaronder scheepvaart, scheepsbouw en havens.
[3] Deze afkorting betekent “Baskisch vaderland en vrijheid” of “Baskenland en vrijheid”.
[4] Zie ook paragraaf 3.6 IMO

wegvervoer en spoorvervoer. Een belangrijk doelgebied voor DGG in dit verband zijn de havens, waarbij het vooralsnog voornamelijk om de "interface" met het schip gaat. In een later stadium zal de haven als geheel door middel van een EU-richtlijn eveneens ter sprake komen. Hiermee wordt dan gelijk het verband met andere vervoersmodaliteiten gelegd, omdat deze in een haven als Rotterdam samenkomen. Dit vindt zijn weerslag in het gegeven dat de Europese Commissie in de tweede helft van 2004 met een ketenrichtlijn "security" denkt te komen. Dit onderzoek beperkt zich echter tot het maritieme cluster, zoals deze reeds is gedefinieerd.

De hierboven genoemde ontwikkelingen zijn van invloed op de bestuurlijke verhoudingen op landelijk, provinciaal en gemeentelijk niveau. Voor wat betreft het maritieme cluster is V&W leidend in het dossier, ondanks het feit dat er sprake is van openbare orde en veiligheid. Dit begrip moet gezien worden in de context van security ten behoeve van het maritieme cluster.

2. Het onderwerp kent facetten die vanuit bestuurskundige optiek interessant zijn

Op terreinen waar V&W geconfronteerd wordt met het nieuwe beleidsterrein security, zal de hele keten van minister tot en met uitvoering, beheer, handhaving en inspectie onder de loep genomen moeten worden. Immers, met het nieuwe beleidsterrein komen zowel nationale als internationale richtlijnen aan de orde die in termen van beleid nadrukkelijk de minister en de ambtelijke (sub)top in beeld brengen en ook aandacht vragen voor de uitvoering die sinds de gebeurtenissen in Enschede en Volendam dominanter op de politieke agenda zijn komen te staan. Voor het zeescheepvaartbeleid kan daar aan worden toegevoegd dat deze politieke agendering van beleid en uitvoering zich niet beperkt tot de nationale grens. Rekening moet worden gehouden dat voor dit specifieke beleidsterrein de Koninkrijksverhoudingen nadrukkelijk in beeld komen.
Zowel conceptueel als materieel vragen de Nederlandse Antillen om hulp bij het opzetten en uitvoeren van een maritiem securitybeleid. Hiertoe zijn zij volgens het Koninkrijksstatuut gerechtigd. Inmiddels is bekend dat de Nederlandse Antillen een eigenstandig haven-securitybeleid voeren, waarbij teruggevallen wordt op de expertise van Rotterdam. Ten aanzien van de schepen die varen onder Antilliaanse vlag, moet vermeld worden dat deze onder de verantwoordelijkheid van het hoofd van de Nederlandse scheepvaartinspectie vallen. Doordat er sprake is van een gelijksoortige benadering in en door de Nederlandse Antillen, wordt dit niet apart uitgediept in dit onderzoek.

3. Nieuwe bestuurlijke verhoudingen

V&W voert overleg met andere departementen over openbare orde en veiligheid voor de beleidsterreinen die V&W aangaan. De hier uit te ontwikkelen wetgeving en bestuurlijke systemen zullen enerzijds onderdeel gaan vormen van het bestuurlijke systeem van V&W, terwijl anderzijds dit ministerie deel uitmaakt van een groter geheel waarin aan openbare orde en veiligheid gedaan wordt.
Als voorbeeld hierbij: De betrokkenheid van V&W bij de Noordzee was voorheen gericht op milieu en veiligheid, maar zal - gegeven de dreiging die vanuit de Noordzee uit kan gaan - raken aan openbare orde en veiligheid. Een ander voorbeeld van de nieuwe bestuurlijke verhouding is dat de minister van V&W taken en bevoegdheden mandateert aan de burgemeester van de desbetreffende haven.

4. Ketenbenadering

De zwakste schakel bepaalt de sterkte van de keten. Met andere woorden: het neerzetten van een securitybeleid binnen het terrein van het maritieme cluster, verliest potentie indien maatregelen in en rondom de haven niet of in onvoldoende mate getroffen worden dan wel niet te treffen zijn. In hoofdstuk 2 wordt middels een aantal theorieën ingegaan op dit aspect. In hoofdstuk 4 is dit punt ook bij de vraagstelling meegenomen

Generiek gezien heeft V&W heeft als hoeder van "Gateway for Europe"[5] een kwaliteitsverantwoordelijkheid ten aanzien van logistieke systemen, welke een belangrijke bijdrage leveren aan het BNP. Binnen V&W wordt een goed securitybeleid gezien als een belangrijk kwaliteitsaspect.

[5] In dit verband wordt hier gerefereerd aan de haveninfrastructuur van m.n. Rotterdam en Amsterdam, die als logistiek centrum voor Europa fungeert.

Nederland moet een betrouwbare handels- en transportpartner zijn. In dit verband wordt onderkend dat maritieme beveiliging een wezenlijke factor in de internationale concurrentieverhouding is geworden. Het bedrijfsleven heeft dit ook erkend en mort grosso modo niet over de te maken kosten, omdat de nieuwe regelgeving zowel mondiaal als europees toegepast moet worden.

1.4 Werkwijze en beperkingen

In dit onderzoek wordt gebruik gemaakt van twee methoden van onderzoek:

Ten eerste wordt middels een literatuurstudie bekeken of er in het verleden vergelijkbare situaties zijn geweest die een antwoord kunnen geven op (een deel) van onderhavige problematiek.

Ten tweede zijn interviews gehouden met respondenten binnen DGG en met respondenten van externe organisaties. De gesprekken zijn gevoerd met personen die uit hoofde van hun functie een relatie hebben met het securitybeleid van DGG. De reden dat niet alleen intern, maar ook extern met betrokkenen is gesproken is dat veel beleid dat door DGG wordt ontwikkeld door externe partijen moet worden uitgevoerd.
Een aantal van de externe actoren die een directe relatie hebben met het securitybeleid van DGG zijn stakeholders/brancheverenigingen zoals de Koninklijke Vereniging van Nederlandse Reders (KVNR), de Nationale Haven Raad (NHR) en de Havenautoriteiten.
Andere externe actoren waarvan de invloed op het securitybeleid van DGG merkbaar is zijn de ministeries van Binnenlandse Zaken en Koninkrijksrelaties (BZK), Buitenlandse Zaken (BUZA), Justitie, Defensie, Volkshuisvesting Ruimtelijke Ordening en Milieu (VROM) en Algemene Zaken (AZ).

1.5 Opbouw

In hoofdstuk 2 wordt het stappenplan van Price als onderzoekskader voor de theorie gebruikt. Hiermee is de structuur van dit hoofdstuk bepaald. De theorieën van Beck, Garland en Perrow worden onder een - aparte en niet door Price benoemde - stap “Waarschijnlijkheid” geclusterd. Aan de hand van een vergaderstuk van de Tweede Kamer wordt de stap “Detectie” gepoogd te verduidelijken. In de stap “Crisismanagement” worden de theorieën van Rosenthal omtrent crisisbesluitvorming besproken. Ook wordt in deze stap ingegaan op de reactie na een terroristische gebeurtenis volgens Rosenthal en ’t Hart en de visie van Douglas & Wildawsky omtrent risicofactoren in het besluitvormingsproces. In de laatste stap staat de herstelperiode volgens Rosenthal en ’t Hart beschreven.

In hoofdstuk 3 (“Securitybeleid op papier”) wordt ingegaan op het fenomeen terrorisme en de relatie met het securitybeleid binnen het maritieme cluster van DGG. Tevens staan in dit hoofdstuk de relevante interne en externe actoren alsmede hun rol bij het securitybeleid van DGG beschreven. De IMO en de Taskforce Security van DGG komen in aparte paragrafen aan bod. Tenslotte wordt in dit hoofdstuk ook ingegaan op het plan van aanpak “Maritieme Security”, waarvan de situatie in Nederland, de strategie van DGG en de sturing/regie onderdeel uitmaken.

In hoofdstuk 4 (“Securitybeleid in de praktijk”) wordt wederom met behulp van het stappenplan van Price de structuur van dit hoofdstuk neergezet. De antwoorden van de respondenten zijn geclusterd volgens dit stappenplan. De eerste stap (Preventie/risico’s) valt uiteen in soorten bedreigingen en soorten maatregelen. In de tweede stap (Detectie) wordt ingegaan op de uitkomsten van inlichtingendiensten en andere relevante organisaties. De derde stap (Crisismanagement) valt uiteen in type besluitvorming, visie op de risico’s en soorten schades. In de laatste stap (Herstel) komen de actoren aan bod die tijdens een herstelperiode van belang zijn. De slotparagraaf van dit hoofdstuk gaat in op een integrale visie op de keten. De communicatie c.q. informatie-uitwisseling staat hierbij centraal.

Tenslotte gaat het slothoofdstuk in op de conclusies en de aanbevelingen die gedurende het onderzoek naar aanleiding van de probleemstelling naar voren kwamen.

2 Theoretisch kader

2.1 Inleiding

Op 11 september 2001 werd de wereld met een nieuwe vorm van buitenlandse terreur geconfronteerd. Kenmerkend daarbij was het gegeven dat een natie op binnenlands territorium een massale aanval onderging. Hier was dus niet zozeer sprake van een oorlog – zonder oorlogsverklaring in traditionele zin – maar ging het om een terroristische actie met een groot aantal kenmerken van een oorlogssituatie. De reactie van de Amerikaanse overheid was navenant en beperkte zich niet alleen tot de eigen natie.
Het ontwikkelen van het security-beleid binnen het maritieme cluster heeft als kern dat de gebeurtenissen van 11 september 2001 in de VS hieraan ten grondslag liggen. Eigenlijk is de term "security-beleid" niet adequaat. In de literatuur wordt securitybeleid gekoppeld aan preventief "veiligheidsbeleid" dat erop gericht is alle denkbare scenario's voor te bereiden en de consequenties daarvan in kaart te brengen.
Crisisbeleid daarentegen, hoezeer het ook een aantal kenmerken heeft van securitybeleid, onderscheidt zich in die zin dat beleid – in eerste aanleg – op ad hoc basis eerst dan wordt geformuleerd, tijdens en nadat een aanval heeft plaatsgevonden.
Het belangrijkste verschil tussen securitybeleid en crisisbeleid is dus gelegen in het gegeven dat het eerste "preventie" als onderscheidend kenmerk heeft en het tweede "nazorg". Tegelijkertijd kan dit onderscheid niet blijvend worden bestendigd. Immers, na een crisis waar in de hectiek van de omstandigheden beleid wordt geformuleerd ontstaat er een periode waarin in betrekkelijke rust, maar nog wel veelal met de nodige politieke aandacht, preventieve maatregelen worden ontwikkeld (= securitybeleid). De gebeurtenissen in Enschede en Volendam en meer recent de Haagse gasontploffing passen naadloos in deze beschrijving. Als men kijkt naar de gebeurtenissen van 11 september 2001 in de VS en de gevolgen hiervan, dan kan men stellen dat het Nederlandse securitybeleid een direct gevolg is van het Amerikaanse crisisbeleid na deze gebeurtenissen op 11 september 2001. Dit geldt met de nodige veranderingen ook voor het maritieme cluster.
Eigenlijk wordt in dit geval ook gesproken over crisisbeleid, met daarbij het grote verschil dat de ramp of aanslag niet in Nederland heeft plaatsgevonden, maar in de VS. Nederland - en dus ook het maritieme cluster - wil voorkomen dat een ramp of aanslag in Nederland zal plaatsvinden. Voorkomen is echter een utopie, maar de kans verkleinen kan wel door ervaringen van anderen (in dit geval: de VS) te gebruiken bij de ontwikkeling van een nationaal securitybeleid binnen het maritieme cluster.
Het crisisbeleid is een onderdeel van de Rijksoverheid dat al sinds de jaren '60 operationeel is. De Cuba-crisis met een internationale uitstraling van een koudeoorlogssituatie gaf een direct impuls aan de ontwikkeling van dit crisisbeleid. In die zin is dus overheidsingrijpen - daar waar het gaat om het bepalen van de doelen, maar zelfs tot en met de uitvoering van de kleinste details - een integraal onderdeel van het ruimere overheidsbeleid. Ieder departement heeft zijn eigen crisisafdeling en de coördinatie daarvan loopt via de DCC's. Op hun beurt zijn het ministerie van BZK, maar zeker ook het ministerie van Defensie de belangrijkste actoren in het veld. De betrokkenheid van het ministerie van Defensie vloeit voort uit het gegeven dat crises voornamelijk vanuit een militaire invalshoek worden bekeken en waarbij in feite het gedachtegoed werd bepaald door een eruptie van de Koude Oorlog (Allison & Zelikow, 1999: 88 – 91).

De begrippen veiligheidsbeleid, securitybeleid en crisisbeleid worden vaak door elkaar gebruikt en bieden geen uitgangspunt voor een theoretisch kader. Price (2004:331) hanteert een stappenplan voor "port security". Dit stappenplan wordt in de volgende paragraaf uitgewerkt.

2.2 Onderzoekskader

Het kader dat in dit onderzoek wordt aangewend om het onderscheid tussen securitybeleid en crisisbeleid te verhelderen is het stappenplan van Price. Dit stappenplan kan goed worden gebruikt als onderzoekskader bij dit hoofdstuk: Price zet de fasen van “port security” uiteen. De achterliggende gedachte van Price bij dit stappenplan is een “life cycle of terror events”.

Stap 1: Preventie/risico’s (paragraaf 2.4)
Barrières opwerpen waardoor het plannen dan wel het laten plaatsvinden van een terroristische actie wordt voorkomen, het minimaliseren van de risico’s op het plaatsvinden van een terroristische gebeurtenis.

In deze stap kan een aantal bedreigingen worden onderscheiden:
- Bedreigingen aan het schip, inclusief lading en passagiers;
- Bedreigingen voor de infrastructuur;
- Bedreigingen voor de omgeving;
- Bedreigingen door het vervoeren van materiaal voor aanslagen.

De maatregelen ter preventie van voornoemde bedreigingen kunnen worden uitgesplitst in:
- Internationale maatregelen;
- Nationale maatregelen;
- Maatregelen op het schip;
- Maatregelen voor reders.

De onderverdeling in soorten bedreigingen en maatregelen wordt in hoofdstuk 4 verder uitgewerkt.

Stap 2: Detectie (paragraaf 2.5)
Pogingen om terroristische aanslagen tijdig te ontdekken en vroegtijdig overgaan tot aanhoudingen.

Stap 3: Crisismanagement (paragraaf 2.6)
Als reactie na het plaatsvinden van een terroristische gebeurtenis achterhalen hoe en waarom deze heeft plaatsgevonden, het verzachten van de impact en het leed van de gewonden, en het mogelijk aanhouden van de verdachten.

Bij deze stap wordt een onderverdeling gemaakt in:
- Type besluitvorming;
- Visie op de risico’s;
- Soorten schades.

Deze onderverdeling wordt in hoofdstuk 4 verder uitgewerkt.

Stap 4: Herstel (paragraaf 2.7)
Het terugkeren naar de dagelijkse gang van zaken door het herstellen en vervolgens het schadeloosstellen van de verliezen.

Price gaat bij zijn stappenplan in op de waarschijnlijkheid (“probability”) van een terroristische gebeurtenis. Hij geeft aan dat het pogen om terroristische aanwijzingen vast te stellen en daarbij te vertrouwen op gebeurtenissen uit het verleden, gebruik makend van inlichtingendiensten, de enige methode is om terroristische gebeurtenissen te voorspellen (Price, 2004: 335). Het gebruik maken van inlichtingendiensten vormt een belangrijke schakel bij de voorspelling van de waarschijnlijkheid van een terroristische gebeurtenis.

Deze koppeling van waarschijnlijkheid aan het gebruik maken van inlichtingendiensten sluit niet één op één aan op een aantal andere theorieën. De theorieën van Beck, Garland en Perrow plaatsen het aspect van waarschijnlijkheid juist in een bredere maatschappelijke context en gaan uit van de waarschijnlijkheid van een terroristische gebeurtenis als gevolg van technologische vooruitgang. Om deze reden kunnen deze theorieën niet onder één van de stappen van Price worden ondergebracht. Deze theorieën gaan meer in op de maatschappelijke context (omgeving), die gekenmerkt wordt door hoog technologische interactieve relaties en de daaraan gekoppelde risico's. Deze theorieën ressorteren eigenlijk in een soort "stap 0" (waarschijnlijkheid), als het ware een omgevings-voorwaarde. In de volgende paragrafen komen de theorieën van Beck, Garland en Perrow aan de orde.

2.3 Waarschijnlijkheid (Stap 0)

In deze paragraaf wordt een aantal theorieën behandeld die ingaan op het aspect van waarschijnlijk-heid van een terroristische gebeurtenis. Deze theorieën koppelen dit aspect niet aan het gebruik maken van inlichtingendiensten, maar zijn allen op zichzelf staande theorieën. Onderstaande theorieën plaatsen het aspect van waarschijnlijkheid juist in een bredere maatschappelijke context en gaan uit van de waarschijnlijkheid van een terroristische gebeurtenis als gevolg van technologische vooruitgang. De risicomaatschappij volgens Ulrich Beck komt in paragraaf 2.3.1 aan de orde en de risicomaatschappij volgens David Garland in paragraaf 2.3.2. In paragraaf 2.3.3 worden de risico's op ongevallen volgens Charles Perrow beschreven.

2.3.1 De risicomaatschappij volgens Ulrich Beck

De Duitse socioloog Ulrich Beck voerde in 1986 voor het eerst de term "risicomaatschappij" in (Beck, 1992). Bij Beck staat dit begrip evenwel niet in het teken van dreiging door bijvoorbeeld terroristische aanvallen. Beck plaatst het begrip risicomaatschappij in een bredere context van een verder doorgeëvolueerde industriële samenleving, waarbij in toenemende mate het private domein verschuift naar het publieke domein. Hij geeft bijvoorbeeld letterlijk aan dat rampen die op het (private) terrein van de fabriek gebeuren, in toenemende mate het publieke domein raken. Beck ziet daardoor een verschuiving van louter privaat naar publiek terrein ontstaan. Deze verschuiving hangt volgens Beck samen met de toegenomen technologische ontwikkelingen en de schaalgrootte waarop deze plaatsvinden.

De stelling van Beck is in principe eenvoudig: de moderne samenleving schiet dramatisch tekort waar het gaat om de onbedoelde gevolgen en risico's die de industriële samenleving voortdurend produceert maar tot nu toe te weinig zag. Volgens Beck is het boemerangeffect van de gevaren van nieuwe ontwikkelingen ingebouwd in het moderniseringsproces zelf. Hij poogt aan te tonen dat ongelukken en gevaren verbonden met technologische projecten inherent onderdeel zijn van de normale bedrijfsvoering en dat ze worden mogelijk gemaakt en gelegitimeerd door de manier waarop we werken en de samenleving hebben ingericht. We gaan met onze risico's om alsof het excessen zijn, maar in feit gaat het om "normale ongelukken". De risicomaatschappij is volgens Beck de onherroepelijke nieuwe fase van modernisering. Een ongeluk als indertijd met de kerncentrale in Tsjernobyl is in zijn ogen een "normaal" ongeluk. Beck stelt dat een dergelijk ongeluk – met wereldomvattende en langlopende gevolgen – eigenlijk een continu ongeluk is, waar we niet eens een goed begrip voor hebben.

De verschuiving van privaat naar publiek – het is al eerder genoemd - is niet zozeer het gevolg van een willens en wetens opgelegde interventionistische politiek, maar komt voor uit het feit dat risico's ten opzichte van bijvoorbeeld tweehonderd jaar geleden zich uitstrekken tot het publieke domein. Men kan zonder de werkelijkheid geweld aan te doen stellen dat er een nieuwe overheidstaak is ontstaan omdat private partijen niet of onvoldoende in staat zijn risico's te beheersen. Voor Nederland zou gesteld kunnen worden dat de grootschalige technologische ontwikkelingen met alle risico's van dien als het ware geleid hebben tot een nieuwe overheidstaak die in het Nederlandse poldermodel zo karakteristiek wordt gemonopoliseerd.

Beck relateert risico's en politiek door te stellen dat een aantal traditionele overheidstaken wordt uitgebreid:

> *"Controlling the market through economic policy, redistributions of income, social security measures – but rather with the non-political: the elimination of the causes of hazards in the modernization process itself becomes political."* (Beck, 1992: 78).

Beck koppelt in zijn benadering heel sterk overheidsoptreden aan risicobeheersing als zodanig. Hij acht dit overheidshandelen onontkoombaar gerelateerd aan de verdergaande technologische ontwikkeling van de westerse maatschappij.
In feite zou - mutatis mutandis – een dergelijke benadering ook kunnen worden toegepast bij dreigingen die opzettelijk worden geuit of worden uitgevoerd. De parallel is dan niet alleen een sterk beroep op de overheid in de vorm van een securitybeleid, maar ook het gegeven dat de moderne technologie ook hier grootschalig kan worden ingezet. In die zin is de analyse van Beck één op één toepasbaar op die van het huidige terrorisme. Immers, nu kunnen zeer grote terroristische aanslagen - zoals die van 11 september 2001 hebben laten zien - worden uitgevoerd als de terroristen kunnen beschikken over middelen waarmee zij toegang krijgen tot technologische toepassingen. De terroristen hadden allen een pilotentraining ondergaan: zij koppelden middelen (geld) aan het verwerven van hoogwaardige, technologische kennis.
Beck analyseert helder en scherp het gegeven dat een hoog technologische maatschappij inherent risicodragend is. Hij geeft evenwel geen antwoord op de vraag hoe als overheid op een dergelijke analyse moet worden geanticipeerd en gereageerd. Voor het begrip van grootschaligheid en verstrekkendheid, is de analyse van Beck echter van groot belang. Het is een illusie te veronderstellen dat onbedoelde ongelukken die voortvloeien uit de huidige technologische ontwikkelingen, zich niet kunnen uitstrekken tot bedoelde "ongelukken", namelijk de terroristische acties die in feite qua reikwijdte dezelfde impact hebben.

De toegang van terroristen of terroristische organisaties tot zowel financiële als technologische middelen doorbreken dit (gewelds)monopolie dat voorheen vrijwel louter aan staten toebehoorden. Daarmee kunnen terroristen grootschalige schade aanbrengen, die historisch toebehoorden aan (legitieme) staten. Zo behoorde bijvoorbeeld het gifgas dat in de Tweede Wereldoorlog, of zelfs in de jaren '80 in Irak werd gebruikt, toe aan geïnstitutionaliseerde entiteiten en niet aan terroristische groeperingen.

Daarmee kan gesteld worden dat wel degelijk lessen getrokken kunnen worden uit de analyse van Beck en het dus zinvol is deze eveneens te betrekken bij de analyse van het securitybeleid van DGG.

2.3.2 De risicomaatschappij volgens David Garland

David Garland analyseert - evenals Ulrich Beck - de risicomaatschappij. In dit onderzoek is het niet de bedoeling om uitsluitend stil te blijven staan tussen verschilpunten van Garland en Beck. Toch mag de analyse van Garland hier niet ontbreken. Garland stelt dat risico een begrip is dat in veelomvattende context geplaatst kan worden.

> *"Today's accounts of risk are remarkable for their multiplicity and for the variety of senses they give to the term. Risk is a calculation. Risk is a commodity. Risk is a capital. Risk is a technique of government. Risk is objective and scientifically knowable. Risk is subjective and socially constructed. Risk is a problem, a threat, a source of insecurity. Risk is a pleasure, a thrill, a source of profit and freedom. Risk is the means whereby we colonize and control the future. 'Risk society' is our late modern world spinning out of control."* (Garland, 2003: 1).

In ieder geval lijkt Garland met deze brede opsomming het begrip risico enigszins te relativeren.
Garland refereert daarbij aan ernstige rampen, zoals Bopal, Tsjernobyl, Three Mile Island (Harrisburg) en ook 11 september 2001.

> *"And it is undeniable that disasters such as Bhopal, Chernobyl, Three Mile Island and September 11th 2001 have shown the appalling injury and destruction that chemical, nuclear or terrorist incidents can bring in their wake."* (Garland, 2003: 28).

Letterlijk vervolgt Garland:

> *"But human societies have always faced massive threats to life and well being – whether from 'nature', in the shape of plagues, famines, floods, and earthquakes, or from other people, as in wars, pogroms and genocides."* (Garland, 2003: 28).

Overigens kan hier worden opgemerkt dat Garland – meer nog dan Beck – uitdrukkelijk ook terroristisch handelen noemt als een risico daar waar hij spreekt over "pogroms" en "genocides".

Voor Garland is de technologische vooruitgang een middel om risico's te beperken. Hij geeft aan dat ook deze tijd wel een oplossing vindt voor de problemen die in dezelfde periode zijn ontstaan. In die zin trekt Garland een minder pessimistische historische lijn door.

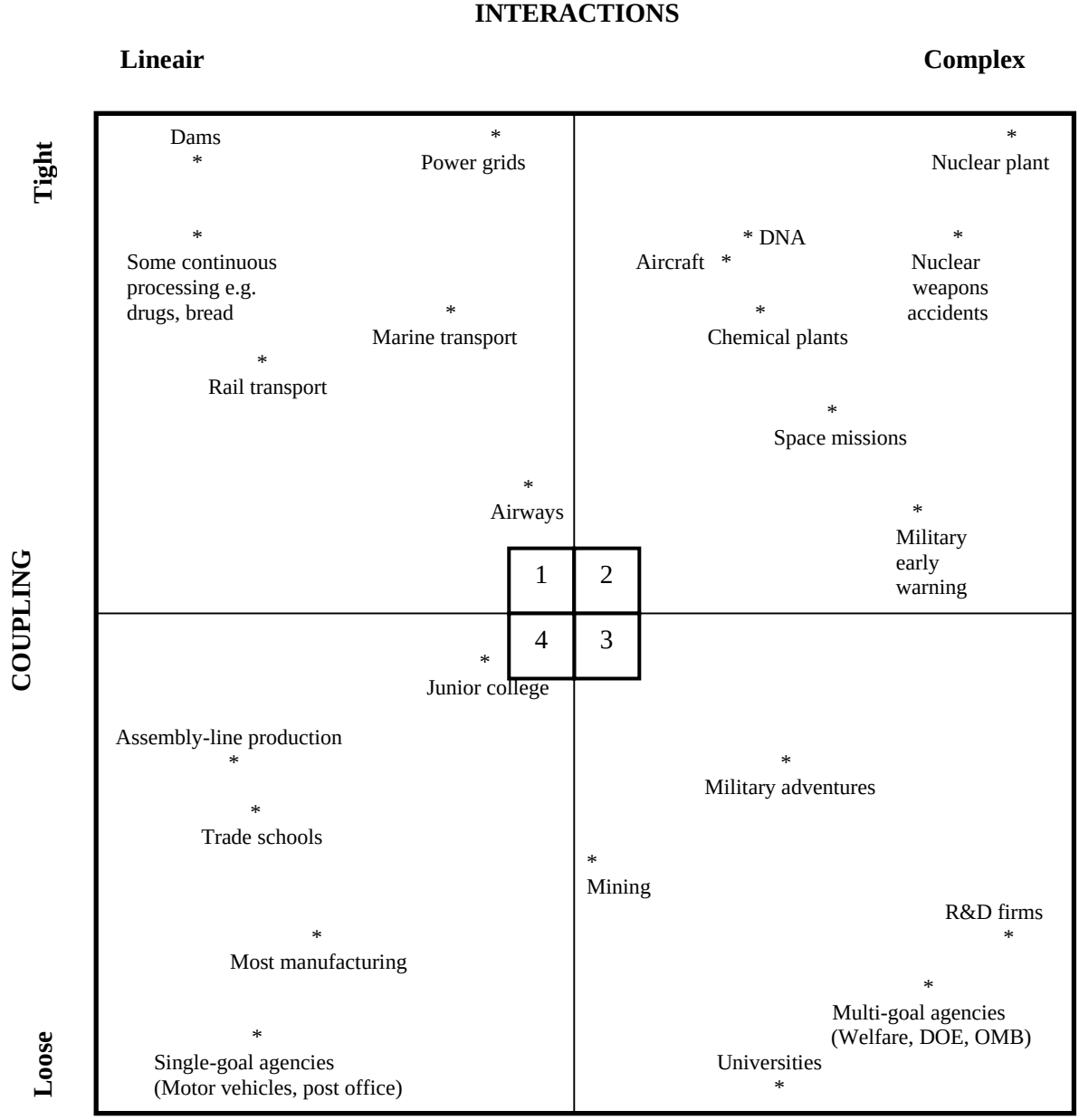
> *"But is not hopelessly optimistic to believe that the same scientific and engineering skills that manufactured these risky processes will be capable of designing technologies and control systems that will manage them effectively, minimizing their misuse, avoiding accidents, and reducing harmful side effects to tolerable levels."* (Garland, 2003: 28).

Met zijn analyse geeft Garland aan dat de risico's van rampen historisch gezien altijd aanwezig zijn geweest. Of het nou aardbevingen, genocide of voedselnood is. In die zin vormt het huidige tijdsgewricht met de nieuwe bedreiging geen uitzondering hierop. Garland geeft aan dat het juist de technologie is die in staat is om effectief de kans op dergelijke "rampen" te verkleinen. In het kader van dit onderzoek is dit een interessante bevinding. Zou - voor zover mogelijk – Beck consequent worden gevolgd, dan kan het terrorisme worden opgevat als een soort ramp die in alle tijden heeft bestaan en geen aanleiding is om al te veel specifieke maatregelen te nemen. Garland is in dit aspect wat uitdagender door te stellen dat juist de technologie oplossingen kan bieden om dit probleem te adresseren. De praktische toepasbaarheid van de analyse van Beck is in dit onderzoek dan ook gering, juist omdat nadrukkelijk technologische oplossingen in beeld worden gebracht.

2.3.3 Risico's op ongevallen volgens Charles Perrow

Charles Perrow beschrijft een aantal ongevallen van zowel de kernenergie-sector, de transportsector, de luchtvaartsector en de sector zeescheepvaart (Perrow, 1984). Opvallend bij zijn analyse is het feit dat hij - evenals Beck - er van uitgaat dat impliciete risico's verbonden zijn aan de hoog technologische samenleving waarin wij leven. Hij analyseert daarbij - meer nog dan Beck - op microniveau en gaat zeer gedetailleerd na hoe ongelukken zijn ontstaan.

Perrow gaat daarbij uit van de door hem geschetste figuur (1984: 97), die hierna staat weergegeven:



Perrow onderzoekt eerst de technische aspecten en vervolgens betrekt hij daarin de menselijke interactie.

In de toelichting van Perrow (1984: 96) over “tight coupling” en “loose coupling” geeft hij de kenmerken weer:

Tight coupling	*Loose coupling*
Delays in processing not possible	Processing delays possible
Invariant sequences	Order of sequences can be changed
Only one method to achieve goal	Alternative methods available
Little slack possible in supplies, equipment, personnel	Slack in resources possible
Buffers and redundancies are designed-in, deliberate	Buffers and redundancies fortuitously available
Substitutions of supplies, equipment, personnel limited and designed-in	Substitutions fortuitously available

In bovenstaande toelichting schetst Perrow zes primaire karakteristieken van “coupling”. Deze karakteristieken kunnen worden onderscheiden – zoals hij het beschrijft – in zowel eenvoudige lineaire verbanden als in complexe verbanden. Zonder nu zelf elk kwadrant exact te beschrijven, geeft Perrow aan dat de afhankelijkheid tussen de variabelen – de mate van “coupling” – in feite het uitgangspunt is van zijn analyse.

Analoog aan bovenstaande redenering kan het begrip “interactions” worden opgezet. Perrow geeft geen definitie van dit begrip, maar refereert in de tekst hieraan met veel voorbeelden. Dit is echter wel voldoende om het onderwerp als “lineair” of “complex” aan te geven.

Overigens geeft Perrow zelf aan dat er op de bovenstaande figuur wel wat valt af te dingen:

> *“The placement of systems is based entirely on subjective judgments on my part”* (Perrow, 1984: 96).

De uitleg van het begrip “interactions” komt het dichtst in de buurt bij het kwadrantenschema van Perrow, zoals dat hierboven is weergegeven. Perrow beschrijft dat dammen, energiecentrales en nucleaire fabrieken met betrekking tot de “coupling” min of meer op één lijn staan, maar dat zij in hoge mate verschillen daar waar het gaat om “unexpected interactions”.

> “While there are few unexpected interaction possible in dams, and not that many in power grids, there are many in nuclear plants.” (Perrow, 1984: 98).

Men zou kunnen stellen dat Perrow “interactions” ziet als handelingen die tot fatale gevolgen kunnen leiden.

Zelf beschrijft hij de lijn lopend vanaf het eerste kwadrant naar het tweede kwadrant als één waarbij de variabelen zeer sterk afhankelijk zijn van elkaar. De in het eerste kwadrant weergegeven dam heeft slechts weinig “unexpected interactions” (Perrow, 1984: 98), terwijl “nuclear plants” - in het tweede kwadrant - zeer veel “unexpected interactions” kent.

Analoog aan de bovenstaande redenering geeft Perrow aan dat bijvoorbeeld postkantoren heel los en lineair aan elkaar gekoppeld zijn. Er zijn weinig “unexpected interactions” en er is voldoende tijd voor

herstel. Ook universiteiten rangschikt hij onder de noemer “loose”, zij het dat Perrow wel stilstaat bij het feit dat dergelijke organisaties beschikken over meervoudige functies zoals onderwijs, onderzoek en dienstverlening richting publiek, maar dat universiteiten in de basis “loose” en “linear” zijn georganiseerd:

> *“It is all quite straightforward, since research and publication are clearly specified as performance criteria for faculty and are outputs of the system.”* (Perrow, 1984: 98).

Perrow laat in dit figuur zien dat er een relatie bestaat tussen het aantal vrijheidsgraden om te handelen en bepaalde hoogwaardige technische processen, zoals die bij een chemische reactie ontstaan.

Daar waar Perrow ingaat op een “verantwoording” van het plaatsen van “Marine transport” in het eerste kwadrant, geeft hij zelf ook aan dat zeker voor deze activiteit ook een ander kwadrant van toepassing kan zijn:

> “On the high seas the system includes the ship, radio communication, the weather, and perhaps one other ship. But as the ship enters a crowded channel, we have not only the weather, but bank effects (the suction created as the ship passes close to the underwater bank of a channel), tides and current flow, wrecks and rocks, bridges, tows and other ships, a crowded radio channel, and navigation lights mixed in with the lights of highways, industrial plants, and distant towers.” (Perrow, 1984: 97).

Gelet op het bovenstaande citaat blijft de plaatsing van “Marine transport” door Perrow in het eerste kwadrant aanvechtbaar. Wordt hier ook zijn omschrijving betrokken van “tight coupling” en “loose coupling” dan is de keuze die Perrow maakt weliswaar verdedigbaar, maar zeker niet voor de hand liggend. Immers, “Marine transport” op de “high seas” moge dan in termen van tijd relatief groot zijn, maar de activiteiten en de variabelen daar waar een schip een haven nadert en daarin verblijft, zijn veelvuldiger en kennen meer onbekende factoren.
De deductie die in dit onderzoek is gemaakt voor het plaatsen van het onderwerp “Marine transport” daar waar het gaat om “coupling” kan met een analoge redenering worden toegepast daar waar het gaat om de beschrijving van een lineaire of complexe interactie. Het moge dan duidelijk zijn dat de situatie op de “high sea” zich zal bevinden in het lineaire kwadrant en de situatie in de havens en omgeving in het complexe kwadrant.

Daarmee wordt de term “Marine transport” – zoals die dit onderzoek wordt uitgelegd – geplaatst in het derde kwadrant van Perrow.

In dit hoofdstuk wordt niet alleen stilgestaan bij de bestuurskundige theorievorming, maar wordt ook gekeken naar de omgevingsfactoren die bij stap 0 aan de orde zijn geweest. Deze analyses kunnen worden opgevat als een raamwerk waarbinnen de bestuurskundige theorieën kunnen worden geplaatst. In die zin vormt deze stap 0 als het ware een inbedding voor het verdere theoretische kader. In hoofdstuk 4 komt - analoog aan deze redenering - dit raamwerk als zodanig niet aan de orde. Dit betekent evenwel niet dat bij de interviewvragen op geen enkele manier hierbij kan worden stilgestaan door de respondenten. Immers, de bedreigingen voor het maritieme cluster maakt integraal onderdeel uit van de vragenlijst.

2.4 Preventie/risico’s (Stap 1)

Een brochure van VNO-NCW (2003: 5) is erop gericht praktische handreikingen te bieden voor crisismanagement voor ondernemers. Deze brochure gaat niet over rampenbestrijding. Evenmin over wat de ondernemer moet doen als het uit de hand loopt. Er wordt vooral gekeken naar de voorbereidingsfase en naar de mogelijkheden om de implicaties van een ernstige situatie te beheersen. Een voorbeeld van een dergelijke ernstige situatie is als volgt:

> "Een groep criminelen dreigt de producten van een frisdrankfabrikant te vergiftigen, als de ondernemer niet over de brug komt met een aanzienlijk bedrag. Bij weigering of politie-inmenging gaan ze over tot het plaatsen van de vergiftigde frisdrank bij grote, drukke supermarkten in de Randstad. Welke acties moeten we direct nemen?"(2003: 13).

In deze brochure wordt het begrip crisismanagement geplaatst in het voorbereiden op situaties:

> "de activiteiten en inspanningen van een onderneming, die als doel hebben zich goed voor te bereiden op situaties die voor de onderneming ernstige inbreuken op de strategisch gewenste gang van zaken kunnen opleveren." (2003: 21).

Echter, in dit onderzoek is crisismanagement uitdrukkelijk voorbehouden aan het ter plekke, tijdens en (direct) na de crisis handelen.

Even verderop in dit boekwerk van VNO-NCW wordt de preventie verder uitgewerkt.

> "door realistische situaties in de crisisscenario's te beschrijven, wordt de voorstelbare praktijk dichtbij gebracht. De scenario's spelen een belangrijke rol bij onder meer de training van het te vormen crisismanagementteam." (2003: 22).

Rosenthal en 't Hart schrijven in het boek "Flood Response and crisis management in Western Europe" het volgende:

> "The dissemination and reception of disaster warnings is a social and not a mechanical process. Three factors are important here: the clarity of the message, the credibility of the source, and the risk perceptions of people." (Rosenthal en 't Hart, 1998: 3).

Bovenstaand citaat sluit zeer goed aan bij het laatst aangehaalde citaat uit het boekwerk van VNO-NCW.

Rosenthal en 't Hart schetsen verder het dilemma van de betrouwbaarheid van de preventie-informatie, daar waar zij spreken over het "cry wolf syndrome". Dit syndroom beschrijft het verschijnsel van het jongetje in het bos dat bij elk geluid dat hij hoorde "cry wolf" riep. Toen de wolf eenmaal daadwerkelijk opdook werd het jongetje niet meer geloofd (Rosenthal en 't Hart, 1998: 4).
Voor een effectief securitybeleid is "awareness" in deze stap een belangrijke voorwaarde. Met het "cry wolf syndrome" wordt aangegeven dat een permanente "overkill" aan "awareness" uiteindelijk zal leiden tot inertie. Dit aspect komt in de vragenlijst[6] aan de orde, daar waar het gaat over maatregelen die respondenten missen bij andere organisaties.

Price gaat hierbij in op het dreigingniveau van een terroristische gebeurtenis en spreekt over een drietal omstreden "Maritime Security Levels (MARSEC)":

> "For cities in general, the confusion and cost of complying with national terror alerts are driving cities to question the whole system… In early June 2003 [Secretary Tom] Ridge acknowledged that states and cities are frustrated with the system, saying that in the future, his agency would try to issue alerts more targeted towards a geographic region or a particular industry." (Price, 2004: 337).

In bovenstaand citaat geeft Price aan dat die bestuurslagen die afhankelijk zijn van centrale informatiebronnen, deze zodanig moeten ontvangen en ontsluiten dat zij er in de praktijk ook iets mee kunnen doen. Een simpele opdeling in kleuren en niveaus, werkt als algemeen middel op het terrein van de "awareness", maar is relatief snel uitgewerkt en biedt autoriteiten ter plaatse onvoldoende handvatten om preventieve taken op zich te nemen.

[6] Zie bijlage 2: Interviewvragen

Nudell en Antokol plaatsen bovenstaand dilemma meer in een statistische context en verwijzen hierbij naar de kans op een natuurramp (1988: 10). De praktische bruikbaarheid van een dergelijke preventiemethode mag dan voor de “probability” van een natuurramp zeer bruikbaar zijn, voor een terroristische aanslag echter, maakt het aantal parameters het aanzienlijk lastiger om deze preventie-methode te hanteren.

Als we hierbij een vergelijking trekken door gebruik te maken van een actueel voorbeeld, kan de mogelijkheid worden genoemd dat Nederland zich zou terugtrekken uit Irak. Waarschijnlijk zou de kans op een terroristische aanslag in Nederland verminderen. In die zin kan dus gebruik worden gemaakt van een meer statistische benadering zoals Nudell en Antokol dit doen.

Een preventieve maatregel die genomen kan worden is dat de betrokken actoren uit het securitynetwerk elkaar goed blijven informeren en helder krijgen wat nu de reële dreigingen zijn. Met andere woorden: actoren moeten voldoende “aware” zijn van de potentiële gevaren.

2.5 Detectie (Stap 2)

Deze stap vloeit logisch voort uit stap 1 en is in feite een handhavingaspect bij de preventie. Geen der behandelde auteurs maakt een expliciet onderscheid tussen preventie en detectie. Ook Price geeft geen toelichting op deze stap, die in feite een verbijzondering is van preventie.

In één van de vergaderstukken van de Tweede Kamer van het vergaderjaar 2003 – 2004 leggen de vaste commissies voor Defensie en voor Binnenlandse Zaken en Koninkrijksrelaties een vraag voor aan de minister van V&W over de brief inzake de nationale signal-intelligence (Sigint)-organisatie.

> Vraag:
> “Biedt de nieuwe opzet van de organisatie voor de interceptie van niet-kabelgebonden telecommunicatie voldoende mogelijkheden om de in het verleden door Nederland verkregen reputatie wat betreft het onderscheppen en decoderen van berichten die van belang zijn voor de nationale en bondgenootschappelijke veiligheid, ook in de toekomst hoog te houden? Vormen Nederlandse capaciteiten in dit opzicht nog steeds een belangrijk voordeel in de ‘voor wat, hoort wat’-benadering binnen de internationale inlichtingenwereld?”
>
> Antwoord:
> “De Nationale Sigint Organisatie (NSO) stelt de MIVD en de AIVD voor de uitvoering van hun wettelijke taken in staat op doeltreffende en doelmatige wijze van hun Sigint-bevoegdheden gebruik te maken. De Wet op de Inlichtingen- en Veiligheidsdiensten-2002 biedt de MIVD en de AIVD de mogelijkheid om zowel gegevens aan buitenlandse inlichtingen- en veiligheidsdiensten te verstrekken als technische of andere vormen van ondersteuning te leveren. Belangrijk daarbij is wel dat de belangen van desbetreffende buitenlandse diensten niet onverenigbaar zijn met die van de MIVD en van de AIVD en dat deze vorm van samenwerking de MIVD en de AIVD niet belemmert bij de uitvoering van hun taken. De aanwezigheid van een substantiële Sigint-capaciteit biedt inderdaad voordelen voor de samenwerking met buitenlandse inlichtingendiensten- en veiligheidsdiensten.” (Tweede Kamer, 2003-2004, 27925 nr. 110).

Bovenstaande vraag en antwoord is een treffend voorbeeld van een poging van de Nederlandse staat (hier: MIVD en AIVD) om terroristische aanslagen op tijd te ontdekken. In dit voorbeeld wordt door gebruik te maken van de nationale Sigint-organisatie de kans op het aanhouden van terroristen groter en daarmee wordt het internationaal terrorisme bestreden.

De groeiende “awareness” voor terrorisme in Nederland (stap 2 van Price) wordt als een serieuze entiteit benaderd. Er is sprake van een nieuwe expliciete detectietaak voor de AIVD.

2.6 Crisismanagement (Stap 3)

Na de gebeurtenissen van 11 september 2001 in de VS is vast te stellen dat op grond van een acute situatie de bestaande – en binnen de organisaties geïncorporeerde – crisisbeheersingsafdelingen werden geactiveerd. Deze revitalisering van deze beheersafdelingen was niet zozeer het gevolg van een goed overdacht en uitgewerkt organisatorisch vormgegeven beleid, doch werd veeleer als een "beter iets dan niets"-situatie – hoe inadequaat ook – ingegeven door de acute politieke realiteit. Immers, zeker onder druk van de media maar ook van de Tweede Kamer moet er handelend kunnen worden opgetreden door een overheid. Dat daarbij dan eerst gekeken wordt naar bestaande structuren en instrumenten is niet alleen voor de hand liggend, maar – gelet op de politieke context – ook geboden. Eerst een nieuwe organisatiestructuur optuigen terwijl er een zeer grote externe dreiging aanwezig is, is niet alleen onzinnig maar zou ook vergaande politieke consequenties hebben.
Het bovenstaande betekent dus dat vanuit een overheid op een volstrekt onverwachte situatie gereageerd kan en – welhaast – moet worden door gebruik te maken van bestaande instituties, netwerken die hieraan verbonden zijn en instanties die gerelateerd zijn en kunnen worden aan de acute situatie. Hoezeer dit ook "for the time being" politiek adequaat moge zijn, voor de langere termijn is het gewenst dat er een structuur ontstaat die niet alleen kan inspelen op acute dreigingen, maar – en wellicht nog veel belangrijker – als belangrijkste taak krijgt deze bedreigingen te voorkomen. Aldus is binnen DGG het securitybeleid tot stand gekomen.

Bij DGG is letterlijk begonnen met het activeren van het sluimerende - wegens het ontbreken van een reële dreiging – crisisbeheersingsbeleid. De gebeurtenissen in september 2001 zorgden ervoor dat terug werd gegrepen naar deze structuur, die - nadat de acute dreigingsituatie achterwege bleef - in feite werd omgevormd tot de structuur die nodig was voor nieuw te creëren beleid, namelijk het securitybeleid van DGG. Centraal bij dit securitybeleid staat immers de preventie in plaats van beheersing achteraf.

Wanneer er wordt gesproken over de besluitvorming die met het ontwikkelen van het securitybeleid is gemoeid, spreek je uiteraard ook over politiek-bestuurlijke besluitvorming. In de bestuurskunde is besluitvorming binnen het openbaar bestuur welhaast het kenobject. Vele theorieën zijn dan ook beschreven, waarin beleidsprocessen al dan niet gedefinieerd worden omschreven. Deze beschrijvingen kenmerken zich grosso modo door een opsomming van interne en externe stakeholders bij besluitvormingsprocessen en door veelal een procesmatige stapsgewijze beschrijving van het proces. Idealiter zou een dergelijke insteek ook het crisisbeleid en het securitybeleid kunnen betreffen. Daar waar het gaat om het beleid dat geformuleerd wordt tijdens een crisis, ontbreekt echter een groot aantal elementen die in een normaal beleidsproces wel aan de orde komen.

> *"Bij een crisis worden ook aan de beschikbare tijd grenzen gesteld. De hulpbronnen, die bij het nemen van een crisisbeslissing worden geactiveerd, zijn derhalve beperkt. In crisistermen geformuleerd: gegeven de begrensde effectiviteit van personele en materiële middelen en gegeven een geringe beslissingstijd, staan crisisbesluitvormers voor het probleem dat zij kwalitatief goede beslissingen moeten nemen terwijl hen de middelen om de beslissingen voor te bereiden ontbreken."* (Rosenthal, 1984: 37-38).

Immers, een belangrijk element dat al dan niet manifest bij de diverse bestuurskundige theorieën wordt besproken is het element tijd. Bij een acute situatie ontbreekt het aan deze factor die ruimte biedt om overwogen – op basis van de beschikbare informatie – doeleinden te formuleren en de daarbij horende middelen aan te wenden.

In politiek-bestuurlijke besluitvorming is het niet ongebruikelijk om een onderscheid te maken tussen routine, complexe en crisisbeslissingen. Routinematige beslissingen zijn de meest voorkomende beslissingen binnen het openbaar bestuur. Voor dergelijke beslissingen zijn veelal standaardprocedures ontwikkeld. Uit empirisch onderzoek blijkt echter tevens dat in routinematige situaties niet alleen regels en voorschriften een bepaalde beslissing voorschrijven, maar dat gewoonten, ervaringen en groepsnormen eveneens een grote rol kunnen spelen.

Rosenthal heeft de volgende veelzeggende zienswijze over de kenmerken van crisissituaties:

> "*crises kenmerken zich door het ontstaan van een ernstige bedreiging en door geringe beslissingstijd"* (Rosenthal, 1984: 37).

Het is deze combinatie van factoren die besluitvorming over theorieën met betrekking tot crises als buitenbeentje behandelt. Immers, juist door het ontbreken van tijd kan niet worden voldaan aan een inventarisatie van actoren, interne en externe stakeholders. Bij de theorieën die door Rosenthal worden behandeld, wordt een aantal factoren onderscheiden. Bij elk van zijn behandelde theorieën blijkt dat er bij het besluitvormingsproces nimmer een zeer enge tijdslimiet als onderscheidend criterium wordt gehanteerd. In alle (door Rosenthal) behandelde bestuurskundige theorieën wordt immers uitgegaan van een mogelijkheid om alternatieven te inventariseren. Kenmerk van een acute crisissituatie is dat de tijdsfactor dermate beperkt is dat van een goede afweging van alternatieven er geen sprake meer kan zijn.

2.6.1 Theorieën van Rosenthal omtrent besluitvorming

Rosenthal onderscheidt een aantal theorieën rondom besluitvorming in crisissituaties. Deze theorieën worden hierna geparafraseerd weergegeven (Rosenthal, 1984: 37 – 47). Analoog aan de werkwijze van Rosenthal wordt hierbij eerst kort ingaan op de algemeen theoretische kenmerken van een benadering en wordt deze vervolgens geplaatst in de theorie over crisisbesluitvorming.

2.6.1.1 Rationeel-synoptische theorie

De rationeel-synoptische theorie van besluitvorming beschrijft de volgende ideaaltypische procedure om tot een beslissing te komen. De besluitvormer:

- kent alle alternatieve mogelijkheden waaruit te kiezen valt;
- kent alle consequenties van elk der genoemde alternatieve mogelijkheden;
- plaatst deze consequenties in een volgorde van voorkeuren;
- kiest die alternatieve mogelijkheid die tot de geprefereerde consequenties leidt (March & Simon, 1958: 137).

Terecht geeft Rosenthal aan dat deze beslissingsprocedure theoretisch tot de beste beslissing leidt. Bovenstaande kenmerken van deze theorie beziend, ligt een dergelijke conclusie ook voor de hand. Immers, een bestuurder zou zich met een dergelijk instrumentarium immer kunnen beroepen op zowel een grote mate van volledigheid in de feiten als een ruime kalender om vervolgens die feiten nauwlettend te inventariseren en uiteindelijk te implementeren.

Crisisbesluitvorming

Rosenthal constateert dat deze rationeel-synoptische beslissingsprocedure voor crisissituaties niet geschikt lijkt te zijn. Uiteraard noemt hij als hoofdoorzaak de geringe beslissingstijd in crisisomstandigheden. Deze is onlosmakelijk gekoppeld aan het gegeven dat het veld van de alternatieven niet volledig in kaart kan worden gebracht. Laat staan het in volgorde plaatsen van voorkeuren, zoals dat als basiskenmerk voor deze theorie wordt gehanteerd.
Daar waar het gaat om de periode nadat een ramp of aanval heeft plaatsgevonden, voldoet de rationeel-synoptische theorie beter. Immers, er is dan meer tijd beschikbaar en de besluitvormers krijgen meer inzicht in de alternatieven en kunnen de consequenties van deze alternatieven beter inzichtelijk krijgen. Voorts kunnen besluitvormers beter prioriteiten toekennen aan de aanwezige alternatieven. Tegelijkertijd zal het – gelet op de aanwezige politiek druk om tot resultaten te komen – echter buitengewoon moeilijk zijn te voldoen aan alle kenmerken van dit model. Als crisisbesluitvormings-model voldoet het dus niet daar waar het gaat om de acute situatie en in beperkte mate daar waar het gaat om de situatie daarna.
Opgemerkt kan worden dat deze conclusie overigens ook van toepassing is op andere beleidsbeslissingen. Deze theorie is een dermate ideaaltypische benadering dat deze ook bij andere besluitvormingsprocessen praktisch nooit volledig kan worden gehanteerd.

2.6.1.2 De optimum-theorie

De optimum-theorie van besluitvorming, vooral door Dror gepropageerd, kenmerkt zich door de volgende accenten:

- bij het besluitvormingsproces worden niet alleen rationele, maar ook buitenrationele elementen betrokken (zoals intuïtie, ervaring en inzicht);
- men streeft beslissingen na die voor de besluitvormers duidelijk batige saldi opleveren;
- in het besluitvormingsproces speelt "meta-policymaking" (besluitvorming over het besluitvormingsproces) een belangrijke rol (Dror, 1968: 154-196).

Tegenover de maximalisatie van de rationeel-synoptische theorie stelt Dror de zijns inziens realistische norm van optimalisering. Het belangrijkste verschil tussen beide theorieën is gelegen in het feit dat de rationeel-synoptische theorie langs strikt logische wegen een modelmatige constructie van de beste beslissing ontwikkelt, terwijl de optimum-theorie een besluitvormingsbenadering beschrijft die veel minder utopisch is.

Crisisbesluitvorming

Rosenthal geeft aan dat deze theorie ogenschijnlijk weinig te bieden heeft voor crisisbesluitvormers. De kennis en personele middelen om tot optimale beslissingen te komen ontbreken in belangrijke mate. Met name het tweede en het derde kenmerk van deze theorie tonen dit ook. Immers, het laten opleveren van een batig saldo veronderstelt dat er tijd gevonden kan worden voor een weloverwogen afweging tussen enerzijds de kosten en anderzijds de opbrengsten. Bij een crisissituatie ontbreekt hiervoor de tijd. In die zin verschilt deze theorie niet wezenlijk van de rationeel-synoptische theorie. Ook meta-policymaking is slechts rudimentair aan de orde bij de beginnende crisissituatie. Een crisisteam zal komen tot een stelsel van primaire afspraken, verantwoordelijkheidsverdeling en terugkoppelingslijnen. Er ontbreekt simpelweg de tijd om een uitvoerig beleidsvormingsproces met daarin alle relevante "checks and balances" te ontwikkelingen. Het eerste punt – daar waar met name intuïtie, ervaring en inzicht aan de orde zijn – is ook voor een acute crisis wel van belang. Voor dit punt kan de door Dror gepropageerde theorie wel opgeld doen. Gaan we hier kijken naar de wat meer lange termijn aspecten van crisisbeleid, dan komen de kenmerken beter uit de verf. In die zin is met name ook het besluitvormingsproces en de ontwikkeling daarvan een punt dat terecht door Rosenthal als belangrijk wordt ervaren. De analyse van zowel de rampen in Volendam en Enschede indiceren dat ook. Tops, Boogers en Brandsen (2003: 35) geven aan dat de rampen in deze steden een extra impuls geven aan de sturingsambitie van het Rijk. Voor het securitybeleid, zoals dit binnen DGG wordt gemaakt zou plaats kunnen zijn voor deze theorie. Immers, met name het niveau van de meta-policymaking – inclusief het betrekken daarbij van de particuliere sector (het al dan niet georganiseerde bedrijfsleven) – is kenmerkend voor de activiteiten die na 11 september 2001 zijn gestart. De tijd die weliswaar relatief beperkt is, is toch voldoende om juist dit punt te adresseren.

2.6.1.3 De theorie van de mixed scanning

De theorie van de mixed scanning (grote lijnen en details) is geformuleerd door Etzioni. Een mixed scanning strategie van besluitvorming ziet er zo uit:

- de besluitvormers inventariseren alle relevante alternatieven die zij en hun staven en adviseurs kunnen bedenken (met inbegrip van die mogelijkheden die niet erg gebruikelijk schijnen);
- de besluitvormers selecteren de alternatieven die op het eerste gezicht bruikbaar zouden kunnen blijken;
- deze alternatieven worden nader (gedetailleerder) onderzocht, waarna verdere selectie volgt;
- deze procedure wordt voortgezet totdat één mogelijkheid resteert;
- de besluitvormers richten de uitvoering van de zo genomen beslissing zodanig in, dat er ruimte blijft voor aanpassingen aan nieuwe informatie (Etzioni, 1968: 286-288).

Etzioni zelf geeft aan dat deze theorie met name bij strategische beslissingen van toepassing kan zijn. Hij heeft zijn bevindingen gebaseerd op praktisch onderzoek naar de militaire verkenning waarin met een groot aantal parameters en varianten zodanig gevarieerd kan worden dat de meest optimale beslissing zich als het ware vanzelf aandient.

Crisisbesluitvorming
Etzioni geeft zelf nadrukkelijk aan dat zijn theorie ook van toepassing is op crisissituaties. Blijkbaar kan hij het tactische – korte termijn – crisisscenario koppelen aan de per definitie lange termijn strategische besluitvorming. Rosenthal geeft aan dat Etzioni als het ware die elementen uit de strategische besluitvorming neemt die ook voor het tactische crisisscenario gerealiseerd kunnen worden. Immers, ook bij een tactisch besluit vindt een scan plaats waarbij parameters – hoe beperkt ook – worden beoordeeld op hun samenhang en individuele merites. Het blijft echter een feit dat het voornaamste element, namelijk de beschikbaarheid van voldoende tijd om te wikken en te wegen, ontbreekt.

2.6.1.4 De theorie van de bevredigende oplossing
De theorie van de bevredigende oplossing, waaraan de naam van Herbert Simon verbonden is, behelst de volgende procedure:

- de besluitvormer haalt een aantal voor de hand liggende alternatieve mogelijkheden voor de dag (alternatieven gebaseerd op ervaringskennis);
- hij bepaalt min of meer wat hij met zijn beslissing(en) wil bereiken (hij stelt zijn aspiratieniveau vast);
- hij kiest het eerste het beste alternatief waarmee het aspiratieniveau gehaald wordt (de bevredigende oplossing) (March & Simon, 1958: 140-141).

Daar waar Etzioni de lat met betrekking tot een voldragen besluit hoog legt, lijkt Herbert Simon de praktijk als uitgangspunt te nemen. Hij geeft aan dat de ervaringscomponent bij besluitvorming een belangrijke rol speelt. Deze ervaringscomponent koppelt hij vervolgens aan het aspiratieniveau van de bestuurders. Het beste alternatief waarmee het aspiratieniveau wordt gehaald, wordt de bevredigende oplossing. Noch door Simon, noch door Rosenthal wordt in dit kader de term opportunisme genoemd. Een dergelijke insteek – gelet op de impliciete koppeling van aspiratieniveau en ervaring – dringt zich echter al wel vrij snel op.

Crisisbesluitvorming
Rosenthal geeft aan dat de theorie van de bevredigende oplossing goed kan worden toegepast bij crisisbesluitvorming. Die conclusie is niet verwonderlijk als men kijkt naar de kenmerken van deze theorie. Immers, daar ligt al in besloten dat de wereld van de besluitvorming allesbehalve ideaal is, zeker in termen van crisissituaties, waarbij tijdnood een belangrijke beperkende factor is .

2.6.1.5 De incrementele theorie
De incrementele theorie van besluitvorming is vooral bekend geworden dankzij Lindblom. Hij heeft aan het incrementalisme ook de minder respectvolle naam “muddling through” (doormodderen) gegeven (Lindblom, 1964: 155-179). Een alledaagse omschrijving luidt “besluitvorming bij stukjes en beetjes”. De incrementele theorie beschrijft de volgende procedure:

- de besluitvormer concentreert zich op bekende, vertrouwde alternatieve mogelijkheden;
- hij oriënteert zich op een marginale verbetering van de bestaande situatie;
- hij geeft ruimschoots aandacht aan de beschikbaarheid van middelen om de marginale verbetering te realiseren;
- hij kiest voor een gedragslijn, die slechts marginaal afwijkt van de bestaande situatie.

Lindblom heeft zijn theorie gebaseerd op de bestudering van het politiek-bestuurlijke proces in de VS. Hij plaatst deze theorie – meer dan de ander hierboven genoemde bestuurskundigen – in een sterkere politieke context daar waar hij spreekt over “checks and balances” en “counterfailing forces”. Het zijn deze politieke harde randvoorwaarden die per definitie beleid incrementeel maken.

Crisisbesluitvorming
Rosenthal geeft aan dat bij crisissituaties wel degelijk gebruik kan worden gemaakt van deze theorie. Daarbij geeft Rosenthal wel als randvoorwaarde dat er onder de beslissers overeenstemming moet zijn over het feit dat de incrementele benadering wordt aanvaard. Op zichzelf is dit een merkwaardige uitspraak van Rosenthal omdat het kenmerk van de theorie van Lindblom beschrijvend is, terwijl Rosenthal hier een meer normatieve richting aangeeft. Een van de kritieke beslissingen die crisisbesluitvormers kunnen nemen, zo schrijft Rosenthal, is de aanvaarding van een incrementele benadering. Hij geeft bij het stukje bij beetje naar zich toetrekken van het initiatief in conflictcrises het voorbeeld van de stap voor stap benadering bij gijzelingen. Rosenthal geeft daarmee impliciet aan dat een dergelijke benadering weloverwogen en op basis van het incrementele model wordt toegepast. Het is een merkwaardige zaak dat Rosenthal de conclusie trekt dat dergelijke kleine stappen voort zouden komen uit de afspraak dat gekozen is voor de incrementele benadering. Hij geeft niet aan dat risicobeperking – in welke vorm dan ook – bij bestuurders prevaleert en dat op basis daarvan stap voor stap wordt gehandeld. Daarnaast gaat Rosenthal niet in op het feit dat bij crisissituaties vaak het geval is dat er grote stappen in zeer korte tijd moeten worden genomen. Het incrementele model schiet in dit geval volstrekt tekort.

2.6.1.6 De theorie van de niet-beslissingen
Volledigheidshalve wordt hier de theorie van Bachrach behandeld (Bachrach en Baratz, 1963: 632-642). Bachrach poogt met deze theorie te verklaren waarom politiek-bestuurlijke instanties soms geen beslissing nemen, hoewel er problemen genoeg schijnen te zijn die om een beslissing vragen. Bachrach geeft aan dat bestendiging van de machtsverhoudingen aanleiding zijn om alternatieven uit de weg te gaan. De besluitvormers willen niets doen. Hoe zeer deze afwachtende houding ingegeven kan zijn om de continuïteit van een bestuurlijke constellatie voort te zetten, hoeft het niet per definitie nadelig te zijn voor de samenleving als geheel. Immers, een aantal problemen lost zich vanzelf op. Kosteneffectiviteit van de theorie van de niet-beslissingen kon daarmee nog wel eens gunstig zijn.

Crisisbesluitvorming
Voor een crisissituatie is dit model moeilijk toepasbaar. Immers, vanuit de publieke opinie is er een zeer sterke roep om beleid, en wel op heel korte termijn. De bestuurders kunnen in de marge op een aantal punten volharden in de niet-beslissingsaanpak, maar zullen dit slechts kort kunnen volhouden. De situatie is dermate urgent dat er op korte termijn gehandeld moet worden. Overigens geeft Rosenthal aan dat bij gijzelingen willens en wetens door een aantal landen gekozen wordt voor deze benadering om daarmee de niet-beslissing als instrument in te zetten waarmee tijd gewonnen kan worden.

Bovenstaand hebben we kennisgemaakt met een beschrijving van de verschillende “fundamentele” theorieën die in de bestuurskunde beschreven zijn. Daarbij is aangegeven dat de ene theorie volstrekt niet van toepassing kan zijn op crisissituaties, terwijl andere theorieën in ieder geval elementen in zich hebben die wel betrokken kunnen worden bij besluitvormingsprocessen tijdens crises.
De reden waarom op het tijdsaspect omtrent het beleid van de crisissituatie sec wordt ingegaan, is gelegen in het feit dat ook – na de acute situatie – het beleid letterlijk vanuit een permanente dreiging onder druk staat, waardoor er gewerkt moet worden onder hoge druk en met een beperkte tijdshorizon. De datum 1 juli 2004 - wanneer de ISPS-code geïmplementeerd moet zijn - is hierbij een duidelijk voorbeeld. Deze beperkte tijdshorizon maakt dat ook in de uitwerking van het crisisbeleid niet voldaan kan worden aan uitgangspunten die hierboven zijn geformuleerd bij de beschrijving van de diverse theorieën. Immers, een aantal van deze theorieën gaat ervan uit dat in voldoende mate informatie en dus tijd gevonden kan worden, die als basis dient voor de ontwikkeling van het securitybeleid.

In deze paragraaf wordt een aantal door Rosenthal beschreven theorieën geplaatst tegen de achtergrond van crisisbeleid. Aangegeven is dat de toepasbaarheid van deze theorieën nauw samenhangt met wat verstaan wordt onder het begrip crisisbesluitvorming. Afhankelijk daarvan kunnen conclusies worden getrokken over de toepassing van de respectievelijke theorieën. In het kader van dit onderzoek wordt de crisisbesluitvorming geplaatst in een kader waarbij ook enige tijd na de

gebeurtenis is inbegrepen. Dit is wel een cruciale toevoeging. Naar mate er meer tijd beschikbaar is kunnen meer theorieën worden "meegenomen" omdat tijd (bijvoorbeeld om alles rustig op een rij te zetten) in een aantal theorieën expliciet wordt genoemd. In hoofdstuk 4 is impliciet uitgegaan van het gegeven dat er enige tijd (dus niet een acute situatie) beschikbaar is bij het opstellen van de vragenlijst. Op basis van deze paragraaf zou de rationeel-synoptische theorie het beste toepasbaar kunnen zijn bij het vierde hoofdstuk. Niet zozeer vanwege de "één op één match" met deze theorie, maar meer omdat de andere theorieën minder toepasselijk zijn.

2.6.2 Reactie na een terroristische gebeurtenis volgens Rosenthal en 't Hart

De reactie na een terroristische gebeurtenis zou moeten zijn dat deze volledig het getroffen of bedreigde gebied bestrijkt, aan een brede waaier van dringende behoeften voldoet en de problemen die zich in de gemeenschap voordoen onderkent. De doeltreffendheid van de reactie is een kwestie van het verlenen van snelle en professionele noodsituatiehulp aan slachtoffers. Dit omvat onder andere het zorgen voor vervoer, het bieden van een schuilplaats, het verlenen van medische zorg, het verlenen van materiële steun en het bieden van psychosociale hulp aan slachtoffers. De doeltreffendheid van verrichtingen bij een noodsituatie is sterk afhankelijk van de kwaliteit van het reactieproces: levering van adequate informatie, coördinatie en logistiek binnen en tussen de partijen. Voorts is de efficiënte reactie na een terroristische gebeurtenis geen kwestie van ambtenaren en openbare agentschappen die autonoom handelen. De officiële reacties kunnen slechts succesvol zijn als zij op basis van realistische verwachtingen over het gedrag van de bevolking in het getroffen gebied te werk gaan en als zij met het zelforganiserend vermogen van de lokale burgers rekening houden.
De reactie is voor de leiding een oefening in het nemen van essentiële besluiten over de toewijzing van middelen en behandeling van slachtoffers en andere partijen. Tevens dient de reactieleiding zich bewust te zijn van enerzijds de sociaal-emotionele afmeting van de terroristische gebeurtenis en anderzijds het belang van materiële en symbolische inspanningen die door autoriteiten worden gemaakt om getroffen gemeenschappen enigszins te helpen met de collectieve spanning die door de terroristische gebeurtenis is veroorzaakt (Rosenthal en 't Hart, 1998: 5).

2.6.3 De vier risico situaties van Douglas & Wildawsky

Douglas & Wildawsky gaan van een meer inductieve analyse uit. Zij gaan uit van een model waarin zij risico als volgt definiëren:

> *"Risk should be seen as a joint product of knowledge about the future and consent about the most desired prospects."* (Douglas & Wilawsky, 1982: 5).

Onderstaand wordt verder ingegaan op de visie van Douglas & Wildawsky omtrent risicofactoren in het besluitvormingsproces.

Douglas & Wildawsky onderscheiden een viertal risico-problemen (Douglas & Wilawsky, 1982: 5), welke hierna in een kwadrantenschema staat weergegeven:

		Knowledge	
		Certain	Uncertain
Consent	Complete	Problem: Technical Solution: Calculation 1	Problem: Information Solution: Research 2
	Contested	Problem: (dis)Agreement Solution: Coercion or Discussion 4	Problem: Knowledge and Consent Solution: ? 3

Hieronder worden de kwadranten kort beschreven:

Kwadrant 1:
Wanneer de kennis zeker is en er sprake is van complete overeenstemming, wanneer er overeenstemming is over doel en alle alternatieven (samen met de waarschijnlijkheid dat een bepaalde gebeurtenis zich voordoet) bekend zijn, is het mogelijk om een programma te schrijven met de best mogelijke oplossing. Het probleem is technisch van aard en de oplossing kan worden berekend.

Kwadrant 2:
Wanneer complete overeenstemming wordt gehinderd doordat de kennis onzeker is, is het probleem dat er sprake is van onvoldoende informatie; daarom wordt de oplossing gezien in het doen van onderzoek. Als we kijken naar de manier waarop overheden omgaan met geschillen over risico's in Europa en de VS, observeren Nelkin en Pollak het volgende:

> *"If lack of confidence is thought to be a problem arising from insufficient technical evidence, then the goal is to ascertain "scientific truth". If the controversy is defined in terms of alienation, a more participatory or consultative system is developed. And if the problem of public consensus is defined in terms of inadequate information, it is assumed that people oppose technologies because they are poorly informed. The task then becomes one of "education"*. (Douglas & Wilawsky, 1982: 6).

Kwadrant 3:
Wanneer de kennis onzeker is en er sprake is van het ontbreken van overeenstemming, zijn dat exact de elementen waarin geïnformeerde personen niet meer weten hoe ze risico's moeten beoordelen en zich daarbij verlaten op "bekende", meer sociaal gevormde waarden en normen.

Kwadrant 4:
Wanneer de kennis zeker is en er sprake is van het ontbreken van overeenstemming, is het probleem dat het uitermate moeilijk is om overeenstemming te bereiken over wat de consequenties zijn en welk belang er aan bepaalde consequenties gehecht moet worden. De oplossing hier is oftewel meer dwangmiddelen gebruiken of meer openstaan voor discussie.

Plaatsing maritieme transport in het kwadrantenschema
Het maritieme transport bekeken vanuit de "high sea"-situatie valt in het eerste kwadrant van Douglas & Wildawsky. Het schip blijft varen van A naar B. Problemen zijn technisch van aard en kunnen via calculatie worden benaderd. Bij het maritieme transport in en rondom de haven – zoals dat in dit

onderzoek centraal staat – ontstaat een ander beeld, zij het dat de indeling daarvan in één kwadrant ook vragen kan oproepen.
In ieder geval lijkt ook het vierde kwadrant van Douglas & Wildawsky af te vallen. Het probleem wordt als zodanig niet bestreden.
Het derde kwadrant waarbij de kennis onzeker is en niet duidelijk is hoe het probleem wordt bestreden, biedt aangrijpingspunten.
Ook voor het tweede kwadrant zou geredeneerd kunnen worden dat het maritieme transport daar van toepassing is, omdat de kennis hier onzeker is en de oplossing wordt gezien vanuit het doen van onderzoek.
Samenvattend kan worden gesteld dat voor het maritieme transport het derde kwadrant nog het meest relevant is voor dit onderzoek.

Met betrekking tot crisisbesluitvorming (weinig tijd, weinig kennis) vallen de kwadranten één en vier op voorhand af. Mogelijk zou vanuit de invalshoek "Consent" onder grote druk kwadrant twee nog kunnen worden aangewend, maar dit doet gekunsteld aan. Indien het tweede kwadrant toch als meest bruikbare zou worden gezien, dan zou dit kwadrant onder de eerste stap van Price kunnen worden geplaatst.
In hoofdstuk 4 zal moeten blijken of het derde kwadrant – dat in theorie de meeste aangrijpingspunten blijkt te hebben - ook door de respondenten (impliciet) wordt genoemd.

2.7 Herstel (Stap 4)

Rosenthal en 't Hart spreken van een herstelperiode die in feite turbulent, controversieel, frustrerend en - op een andere manier dan bij stap drie - net zo traumatisch kan zijn. Mensen die geëvacueerd zijn keren terug naar hun huizen, winkeliers openen opnieuw hun deuren en schoonmaak- en reparatiewerk begint op kleine schaal. Het collectieve stressgevoel is allesbehalve verdwenen: een aanzienlijk aantal slachtoffers en reddingswerkers is lichamelijk gewond of lijdt aan posttraumatische stress. Juist deze mensen hebben medische en psychosociale zorg nodig. Uit rampenonderzoek is bekend dat direct nadat de ramp heeft plaatsgevonden de zorg en aandacht veel intensiever en beter voorbereid moet zijn dan de zorg en aandacht op de lange termijn.
In de herstelperiode zullen allerlei betrokken organisaties een onderzoek starten en de crisis evalueren. Het evaluatieproces vindt op verschillende manieren en niveaus plaats. In de politieke arena zullen politieke leiders hun beleid uitleggen en verdedigen en een aantal leerpunten introduceren. Een meer gedetailleerd proces vindt plaats op het operationele niveau waar interne rapporten en "debriefing"-sessies de belangrijkste stimulansen zijn teneinde de nodige leerervaring op te doen (Rosenthal & 't Hart, 1998: 9-10).

Hetgeen Rosenthal en 't Hart hierboven schetsen sluit goed aan bij de visie van Price. Het is echter opmerkelijk dat zowel Price als Rosenthal en 't Hart het herstel niet geëxpliceerd hebben voor herstel in bestuurlijke zin: een relatie leggen tussen enerzijds de terroristische gebeurtenis en anderzijds het tegelijkertijd voorkomen van een dergelijke gebeurtenis. Dus in feite een stap die voorafgaat aan preventie en die de preventie op een hoger plan brengt omdat meer inzicht in de dreiging is ontstaan. In dit kader kan de ISPS-code opgevat worden als een herstelmaatregel ter voorkoming van vervolgschade.

2.8 Afsluiting

Dit theoretisch kader heeft het analysemodel van Price als uitgangspunt genomen. Grosso modo kan gesteld worden dat dit model als onderzoekskader goed voldoet, omdat de door Price genoemde elementen eenduidig en helder zijn beschreven, zodanig dat deze kunnen worden aangewend bij andere in dit hoofdstuk onderzochte theorieën. De sociologische context die uitdrukkelijk niet door Price wordt behandeld - hij hanteert hem als impliciet gegeven – is in dit hoofdstuk besproken aan de

hand van Perrow, Garland, Beck en in mindere mate Douglas & Wildawsky. De hier besproken theorieën vormen in feite een basis die de overige theorieën aanvullen en in een duidelijke context plaatsen.

Met betrekking tot preventie/risico zijn de mate van en de soort bedreigingen aspecten die in hoofdstuk 4 aan de orde komen. Daarnaast laat de analyse van Douglas en Wildawksy zien of dergelijke informatie ("knowledge") zeker of onzeker is en of hierover overeenstemming bestaat onder de respondenten. In hoofdstuk 4 zal vanuit dit perspectief de empirie worden getoetst. Voorts worden de volgende kernvragen beantwoord: Welke bedreigingen worden gezien, welke voorgestelde maatregelen worden afdoende gevonden en welke maatregelen moeten nog samen met DGG worden doorgevoerd?

Het onderscheid tussen detectie en preventie wordt in dit theoretische hoofdstuk niet gemaakt. Voor zover mogelijk wordt dit onderscheid wél meegenomen in hoofdstuk 4.

In dit hoofdstuk is stilgestaan bij het begrip crisismanagement. Aangegeven is dat het van cruciaal belang is dat het element tijd goed moet worden gedefinieerd. Vanuit dit gegeven kwam de rationeel-synoptische theorie als meest voor de hand liggend in aanmerking. In hoofdstuk 4 komen impliciet de door Rosenthal behandelde theorieën aan de orde.

Opmerkelijk is dat Rosenthal en 't Hart uitsluitend spreken over het fysieke herstel en dit koppelen aan begrippen als trauma's. De stappen die Rosenthal en 't Hart bij het evaluatieproces onderscheiden, zoals het uitleggen en verdedigen van beleid en het introduceren van een aantal leerpunten, komen verder in dit onderzoek dan ook niet meer aan bod. Wel kan herstel worden opgevat als een stap voorafgaand aan preventie. Daarmee wordt preventie op een hoger plan gebracht, omdat meer inzicht in de dreiging is ontstaan.

3 Securitybeleid op papier

3.1 Inleiding

In het vorige hoofdstuk is binnen het theoretisch kader een aantal auteurs behandeld volgens het stappenplan van Price. Daarmee is slechts een deel van het formele kader afgedekt. In dit hoofdstuk komt het andere formele deel aan de orde, namelijk hoe het securitybeleid op papier is georganiseerd. In paragraaf 3.2 wordt terrorisme nader bekeken. De relatie tussen terrorisme en het securitybeleid staat in paragraaf 3.3 beschreven. De beschrijvingen van de relevante interne actoren en externe actoren en hun rol bij het securitybeleid van DGG staan weergegeven in respectievelijk paragraaf 3.4 en 3.5. In paragraaf 3.6 wordt de IMO belicht en in paragraaf 3.7 de Taskforce Security van DGG. Het plan van aanpak "Maritieme Security" dat een gevolg is van de ontwikkelingen na 11 september 2001 wordt in paragraaf 3.8 beschreven.

3.2 Terrorisme nader bekeken

Gelet op het groot aantal uiteenlopende definities van het woord terrorisme is het van belang dat in dit onderzoek de definiëring van "terrorisme" wordt besproken, de geschiedenis van het terrorisme kort wordt aangestipt en tot slot wordt ingegaan op de bestrijding van het terrorisme.

3.2.1 Terrorisme

Er bestaat geen eenduidige definitie van het woord terrorisme. Voor een deel hangt dit samen met het feit dat er een subjectieve lading aan het woord terrorisme verbonden is. Wat vanuit het oogpunt van het slachtoffer een terroristische aanslag is, is vanuit het oogpunt van de dader een gerechtvaardigde actie in een vrijheidsstrijd. In de nasleep van de aanslagen op het WTC en het Pentagon in respectievelijk New York en Washington bestempelden veel regeringen de "vrijheidsstrijders" in eigen land als "terroristen". De Russische president Poetin gebruikte de aanslagen om meer begrip te kweken voor zijn harde aanpak van de Tsjetsjeense rebellen. Het dossier terrorisme (2003) is verkrijgbaar via het Internet.
In een rapport van de voormalige Binnenlandse VeiligheidsDienst (BVD) wordt verwezen naar een studie van de universiteit van St. Andrews waarin maar liefst 109 verschillende definities van terrorisme staan vermeld (Hoffman, 1998).

De Binnenlandse Veiligheidsdienst (BVD) heet tegenwoordig Algemene Inlichtingen- en Veiligheidsdienst (AIVD). Deze naamswijziging vloeit voort uit de nieuwe Wet op de Inlichtingen- en Veiligheidsdiensten (WIV) die op 29 mei 2002 in werking is getreden. De WIV 2002 is de wettelijke basis voor het optreden van de AIVD en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD), voorheen de Militaire Inlichtingendienst (MID). Deze wet vervangt die uit 1987.
Met deze wet wordt beoogd te voldoen aan de eisen die het nationale en internationale recht stellen. Zo vloeit uit het Europees Verdrag van de Rechten van de Mens (EVRM) voort dat het werk van inlichtingendiensten voorzienbaar en kenbaar moet zijn voor de burger. De regering heeft deze transparantie tot leidraad gemaakt van de WIV 2002. In de WIV zijn taken en bevoegdheden opgenomen die noodzakelijk zijn voor het goed functioneren van AIVD en MIVD in deze tijd.

De AIVD hanteert als definitie van terrorisme:

> *"Het plegen van of dreigen met op mensenlevens gericht geweld, met als doel maatschappelijke veranderingen te bewerkstelligen of politieke besluitvorming te beïnvloeden."* (BVD, 2001: 9).

De AIVD kiest voor deze smalle definitie waarbij als onderscheidend element ten opzichte van andere gewelddadige aanslagen en activiteiten het doelbewuste streven naar menselijke slachtoffers of het

nadrukkelijk incalculeren daarvan geldt. Een ander onderscheidend element wordt gevormd door het feit dat terroristische aanslagen worden gebruikt om politieke of maatschappelijke veranderingen te bewerkstellingen. Vaak wordt daarbij een psychologisch effect beoogd dat veel verder reikt dan de directe slachtoffers. Terrorisme (in het Latijn betekent terror angst) is erop gericht in een brede kring onrust of paniek te zaaien. De aanslagen in de VS op psychologisch zeer belangrijke financiële en militaire centra en de miltvuur besmettingen daarna voldoen geheel aan deze omschrijving. Relatief nieuw is het feit dat geen organisatie of land de verantwoordelijkheid voor deze aanslagen heeft opgeëist. Daarmee is er een nieuwe vorm van terrorisme ontstaan, waarbij niet een direct en concreet doel wordt beoogd, maar waarbij een terroristische organisatie vanwege religieuze of ideologische redenen zoveel mogelijk slachtoffers wil maken. Het dossier Terrorisme (2003) is verkrijgbaar via het Internet.

3.2.2 Geschiedenis van het terrorisme

Het terrorisme zoals wij dat nu kennen heeft zijn oorsprong in het anarchisme, dat aan het einde van de negentiende eeuw zijn hoogtepunt bereikte met de aanslag op tsaar Nicolaas de Tweede. In deze traditie staat ook de Duitse Baader-Meinhof-groep in de jaren zeventig van de twintigste eeuw. In deze eeuw wordt terrorisme steeds meer een middel dat gebruikt wordt door nationalistische groeperingen die streven naar onafhankelijkheid. De Baskische afscheidingsbeweging ETA en de IRA zijn hiervan de bekendste voorbeelden. Het dossier Terrorisme (2003) is verkrijgbaar via het Internet.

ETA

De ETA is in 1959 opgericht met als doel een onafhankelijk thuisland te vestigen in de Noord-Spaanse gebieden Vizcaya, Guipuzcoa, Alava en Navarra en in de zuidwestelijke Franse gebieden Labourd, Basse-Navarra en Soule. Ze willen dit doen op basis van de Marxistische leer.[7]
De leden hebben in de eerste plaats bomaanslagen en moorden op ambtenaren op hun geweten. Hierbij doelen ze vooral op mensen van de beveiliging in Spanje, op militairen, politici en op mensen van de rechtbank. De ETA komt op verschillende manieren aan geld voor de activiteiten, bijvoorbeeld door middel van gijzelingen, bankberovingen en afpersing. De groep heeft, sinds het begin met dodelijke aanslagen in 1960, meer dan 800 mensen om het leven gebracht. In november 1999 brak de ETA haar "eenzijdige en onbepalende" staakt-het-vuren. Ze begonnen een moord- en bomaanslagenactie, waarbij minstens 23 mensen omkwamen. Meer informatie over de ETA (2003) is verkrijgbaar via het Internet.

IRA

De IRA is een radicale terreurgroep die in 1969 als de bewapende vleugel van Sinn Fein is gevormd. Sinn Fein is een politieke beweging toegewijd aan het verwijderen van Britse militaire krachten uit Noord-Ierland en Ierland. Bovendien willen ze dat Noord-Ierland bij Ierland gaat horen. De IRA heeft een Marxistisch grondbeginsel.
Bomaanslagen, sluipmoorden, gijzelingen, uitbuiting en overvallen: ze behoren allemaal tot de gepleegde daden van de IRA. Doelen waren oudere ambtenaren van de Britse regering, Britse militairen, Britse politie in Noord-Ierland en Noord-Ierse regeringsgetrouwe paramilitaire groepen. Bomaanslagen zijn gepleegd op trein- en ondergrondse stations. Ook pleegde de IRA bomaanslagen in winkelstraten in Groot-Brittannië, op Britse en Royal Ulster Constabulary-doelen in Noord-Ierland en op een Britse militaire instelling op het Europese vasteland. De IRA neemt sinds juli 1997 een staakt-het-vuren in acht. Dat deed de groep ook eens eerder, van 1 september 1994 tot februari 1996. Meer informatie over de IRA (2003) is verkrijgbaar via het Internet.

3.2.3 Bestrijding van het terrorisme

Waar terroristische groeperingen samenwerken om de effectiviteit van hun acties te vergroten, zoeken regeringen over de hele wereld steun bij elkaar om het terrorisme effectief te kunnen bestrijden. De al eerder genoemde spraakverwarring over wat terrorisme nu eigenlijk is, heeft dit lange tijd in de weg gestaan. De eerste poging om in internationaal verband te komen tot een samenwerkingsverband vindt reeds in 1937 in Genève plaats. Pas in 1977 lukt het om op Europees niveau een conventie voor

[7] De leer van Karl Marx, die zegt dat de productiemiddelen in het bezit van de arbeiders moeten komen.

bestrijding van terrorisme aan te nemen. Een week voor de aanslagen in de VS werd in het Europees Parlement overeenstemming bereikt over intensievere samenwerking op het gebied van terrorismebestrijding. De nieuwe maatregelen omvatten onder meer een plan voor een gezamenlijk opsporings- en arrestatiebevel en voor afschaffing van de formele uitleveringsprocedures voor terroristische misdrijven. Naast regeringen en inlichtingendiensten werken ook politiecorpsen samen in organisaties als Interpol en Europol om te proberen grip te krijgen op terroristische organisaties. De "internationale alliantie tegen terrorisme" die de Amerikaanse president Bush aan het vormen is, zal wellicht naast een militaire, ook een juridische en politieke stimulans geven aan de bestrijding van terrorisme. Het dossier Terrorisme (2003) is verkrijgbaar via het Internet.

In de vernieuwingsagenda voor de presterende overheid (Docters van Leeuwen, Deetman, Opstelten, Pastors en in 't Veld, 2003: 21) staat vermeld dat door betere informatie-uitwisseling meer gevoel van veiligheid wordt gecreëerd. Terrorisme kan worden bestreden doordat men over meer integrale informatie beschikt. Hierdoor lijkt de veiligheid in de VS verhoogd. Door deze verbeterde informatievoorziening is men beter in staat risico's in te schatten en terrorisme op te sporen en te bestrijden. Daarnaast heeft de werkwijze een maatschappelijk effect. Op de langere termijn kan er een groter gevoel van veiligheid onder de burgers van de VS ontstaan en krijgt men meer vertrouwen in het functioneren van de veiligheidsdiensten.

3.3 Relatie tussen terrorisme en het securitybeleid

Securitybeleid is een rechtstreeks gevolg van het feit dat er terrorisme op deze wereld bestaat: van security zou een preventieve werking uit moeten gaan om terrorisme in de hand te houden. De diverse aspecten van de samenleving worden geconfronteerd met het fenomeen terrorisme en behoeven derhalve een beleid op het terrein van security. Transport is zeer moeilijk te beschermen en is daardoor haast per definitie in zijn algemeenheid kwetsbaar voor terrorisme, waarbij de mondiaal opererende transportmodaliteiten (zeevaart en luchtvaart) aan het meeste gevaar blootstaan. Met name de VS zijn deze mening toegedaan.

De VS neemt een aanzienlijk deel van de internationale handel voor haar rekening en is - mede gegeven de politieke situatie - extra kwetsbaar voor terrorisme. Het onderwerp van dit onderzoek betreft de modaliteit zeescheepvaart, en het maritieme cluster in het verlengde daarvan. Door Amerikaanse politieke druk is het aandachtsterrein van dit onderzoek als prioritair aangemerkt en is het samen met de luchtvaart speerpuntbeleid in het securitybeleid.

3.3.1 Achtergronden

Inmiddels is het een geaccepteerd gegeven dat de Koude Oorlog van weleer is overgegaan in een situatie die wellicht nog complexer is: vroeger was de opponent duidelijk zichtbaar en eenduidiger te identificeren, waarbij tegenmaatregelen voornamelijk van militaire aard, dan wel gebaseerd op een bepaalde balans waren. Thans is de bedreiging ondergronds, globaal en nauwelijks te determineren, waarbij de objectieven eveneens diffuus zijn en er geen sprake meer is van een rationele balans. Vroeger waren civiele maatregelen veelal gericht op het beperken van de gevolgen van een conflict, terwijl momenteel het accent meer gelegd wordt op preventie.

Tegen de achtergrond van onvoorspelbaarheid qua aard en plaats van de dreiging moet de nieuwe rol van de VS gezien worden: hun rol van hoofdpilaar voor de NAVO is omgezet in die van "politieagent van de wereld", welke zich na 11 september 2001 niet meer beperkt tot het bestrijden van brandhaarden. Het politieke klimaat in de VS uit zich in een enorme inspanning jegens terrorisme, waarbij ook veel geëist wordt van de rest van de wereld. Het nieuwe element hierin is het feit dat er met name iets gevraagd wordt van de civiele autoriteiten. De feitelijke dreiging en de politieke druk zijn zodanig dat deze niet meer genegeerd kunnen worden.

Op 13 november 2002 wordt de "Homeland Security Act 2002 (HR5005)" door het Huis van Afgevaardigden aanvaard en op 19 november door de Senaat. Het Huis heeft op 22 november met

enkele kleine technische aanpassingen ingestemd. Vervolgens is de “Homeland Security Act” op 25 november ondertekend door President Bush. Deze “moeder” van alle “Security Acts” heeft als doel de nationale veiligheid in de VS te handhaven door voorzieningen te treffen waardoor aanslagen op de VS voorkomen kunnen worden (Nederlandse Ambassade te Washington, 2002: 6).

Tom Ridge, die de President in 2002 heeft geadviseerd op homeland defensiegebied, zwaait vanaf 24 januari 2003 de scepter over het “Department of Homeland Security”. Bij dit “mammoet-departement” zijn ongeveer 170.000 mensen werkzaam.

De vorming van dit nieuwe Amerikaanse ministerie betekent een aderlating voor het “Department of Transportation (DOT)”, dat de – begin 2001 opgerichte – “Transportation Security Administration” (waarin al onderdelen van de Federal Aviation Administration, Maritime Administration, Federal Railroad Administration en Federal Highway Administratrion waren opgegaan) en de “US Coast Guard” moest afstaan. Ook de “Immigration and Naturalization Service” en “US Customs” gaan naar het “Department of Homeland Security”. De taak van dit ministerie is de bescherming van het Amerikaanse “thuisland” in alle aspecten: grensbewaking, havens, transport, infrastructuur. Dit ministerie moet uit diverse bronnen de “homeland security intelligence” bijeenbrengen en analyseren. Het moet alle communicatie over terreurdreigingen en de voorbereidingen daarop coördineren met de staten en lagere overheden, met industrie en private ondernemingen en naar het Amerikaanse volk toe. Een volledige tekst omtrent dit nieuwe Amerikaanse ministerie (2003) is verkrijgbaar via het Internet.

Het “Department of Homeland Security” heeft een drieledige missie:
1. Het voorkomen van terroristische aanslagen binnen de Verenigde Staten;
2. Het verminderen van de kwetsbaarheid van de Verenigde Staten voor terrorisme;
3. Het minimaliseren van schade en het herstellen van de gevolgen van de aanslagen die gepleegd kunnen worden.

Speciaal voor de maritieme sector nam de Amerikaanse Senaat op 2 augustus 2001 een wet aan, getiteld “Port and Maritime Security Act 2001 (S1214)”. Deze wet voorzag in een extra-territoriale werking voor wat betreft in buitenlandse havens uit te voeren veiligheidsinspecties van goederen met een Amerikaanse haven als bestemming. Vooruitlopend op deze wet heeft de Amerikaanse douane een “Declaration of Principles” getekend met een aantal landen (waaronder Nederland), op basis waarvan in geselecteerde grote havens in die landen Amerikaanse douane-inspecteurs voor de VS bestemde ladingen mogen controleren.
Na de gebeurtenissen van 11 september 2001 is de wet drastisch uitgebreid om nieuwe bedreigingen van terrorisme ten aanzien van Amerikaanse havens het hoofd te kunnen bieden. Deze nieuwe wet “Maritime Transportation Security Act 2002 (S1214)” werd gesteund door de regering Bush op 6 december 2001 en is unaniem aangenomen door de Senaat op 20 december 2001. De wet is vervolgens op 4 juni 2002 goedgekeurd door het Huis van Afgevaardigden.

3.3.2 Status quo in het maritieme cluster

Logischerwijs is de luchtvaarttak het eerste in beeld gekomen. Door de structuur van de sector en de historie, gevoegd bij extra (financiële) inspanningen, is hier snel resultaat geboekt door het nemen van unilaterale maatregelen, waarbij de luchtvaartsector eenzijdig gedwongen werd bepaalde maatregelen te nemen die de toegang tot de VS zeker moeten stellen. De toekomst zal leren of de maatregelen inderdaad effectief zijn. Vervolgens is door de VS de maritieme sector (zeescheepvaart en havens) als tweede prioriteit in beeld gebracht.

Doordat de maritieme sector eveneens een mondiaal opererende bedrijfstak is zijn vele overeenkomsten met de luchtvaart te signaleren, maar ook vele verschillen:
1. Het luchtvaart cluster is security-technisch beter af te bakenen dan het maritieme cluster. Luchtvaart-verkeer vindt tussen beperkte geografische locaties plaats;
2. De reizen van vliegtuigen worden beter gecontroleerd dan die in de scheepvaart;
3. De informatie-uitwisseling is in de luchtvaart beter geregeld, zowel bij vervoer van passagiers als bij goederentransport;

4. Security speelt in de luchtvaart al langer een belangrijke rol;
5. Er is beter zicht op de verladers in het luchtvervoer;
6. In het luchtvervoer is sprake van betere ladingcontrole;
7. Transparantie in eigendomschap van schepen en lading is in de scheepvaart ver te zoeken (Flags of Convenience: goedkope registers met lagere kwaliteitseisen);
8. Scheepvaarthavens zijn vaak niet besloten: een vrijer verkeer van goederen en personen levert een hogere kwetsbaarheid op, met een grotere kans op aanslagen, en grotere maatschappelijke en economische gevolgen (vb. nabij liggende chemiefabriek die wordt aangevallen).

Deze verschillen maken het security-probleem in de scheepvaart vele malen groter dan in de luchtvaart.

Gekozen is voor een internationale aanpak via:

- IMO: een orgaan van de VN;
- International Labour Organisation (ILO): eveneens een VN-organisatie;
- Europese Unie (EU);
- NAVO;
- Organisatie voor Economische Samenwerking en Ontwikkeling (OESO);
- Groep van de 8 leidende industrielanden (G8)[8].

De ontwikkelingen in IMO hebben geresulteerd in internationale regelgeving op het terrein van security van schepen en terminals (zowel vervoer van goederen als passagiers). Deze regelgeving wordt op 1 juli 2004 van kracht.

Het voordeel van internationale regelgeving is dat dit de grootste kans geeft op een internationaal "Level Playing Field" voor zowel schepen als havens, waarmee oneerlijke concurrentie wordt tegengegaan. Dit is een belangrijk uitgangspunt van het Nederlandse en Europese beleid. Belangrijke voorwaarde hierbij is het aanwezig zijn van controle- en sanctiemechanismen. Deze ontbreken echter: er is wel sprake van moreel sociale druk en van zware economische druk, maar de IMO heeft geen juridische instrumenten om sancties op te leggen.

De Amerikanen ontwikkelen - naast nationale - ook andere initiatieven, welke te maken hebben met de vervoersketen in zijn algemeenheid, toegespitst op containers, welke een belangrijke bedreiging kunnen zijn. Deze initiatieven zijn niet alleen bilateraal, maar ook gericht op de mondiale transportwereld. Uit dit bovenstaand moge blijken dat er een grote mate van internationalisering van dit probleem is. Alle relevante internationale gremia hebben immers het securityprobleem geagendeerd, terwijl naast deze internationale "aandacht" de VS met unilaterale initiatieven komt die de facto gelijk zijn aan die van de internationale gremia. Dit betekent dat ook DGG zeer sterk te maken krijgt met zowel de internationale component als ook de "unilaterale" acties vanuit de VS. Naast uiteraard de nationale aandacht, die zich binnen DGG concentreert.

3.4 Beschrijving relevante interne actoren en hun rol bij het securitybeleid van DGG

In deze paragraaf worden de interne actoren beschreven die een belang hebben bij het securitybeleid van DGG. Hierbij kan niet ontkomen worden aan het zichtbaar maken van de overkoepeling van V&W, welke met name terug te vinden is in het Departementaal Coördinatie Centrum (DCC) van V&W. Alle vermelde actoren hebben in meerdere of mindere mate bemoeienis met security. Doordat ook security niet ontkomt aan een ketenbenadering, zijn er altijd wel raakvlakken denkbaar tussen de verschillende beleidsterreinen van V&W. Als voorbeeld hierbij: de kwetsbaarheid van de infrastructuur is een regelrecht belang voor de diverse transportsectoren van DGG, terwijl er ook onderlinge samenhang tussen die vervoersectoren is.

[8] Tot de G8 behoren de landen: Canada, Verenigde Staten, Frankrijk, Italië, Duitsland, Japan, Verenigd Koninkrijk en Rusland.

- **V&W**

Missie V&W

V&W staat voor het volgende: Nederland duurzaam beschermen tegen water en zorgen voor veilige verbindingen van internationale kwaliteit.

De kerntaken van V&W zijn:

- het ontwikkelen van beleid voor verkeer en water en zorgen dat dit beleid wordt uitgevoerd en gehandhaafd;
- zich richten op de bereikbaarheid, veiligheid en leefbaarheid;
- het rekening houden met eigen verantwoordelijkheden van burgers, bedrijven en andere overheden;
- het ruimte bieden aan medewerkers om hun talenten te ontwikkelen en in te zetten.

Alle sectoren van V&W zijn gericht op veiligheid, kwaliteit en hebben infrastructurele aspecten in zich.

Alle beleidsterreinen van V&W ontkomen niet aan de noodzaak van het voeren van een securitybeleid. Hiertoe is bij DGG een departementsbrede Taskforce externe veiligheid opgericht. Dit onderzoek richt zich echter niet op de departementale externe veiligheid.

Ten behoeve van de security van het maritieme cluster is bij DGG een Taskforce Security opgericht, die zich specifiek op dit terrein begeeft, maar eveneens onder de departementale Taskforce externe veiligheid valt. Deze Taskforce beperkt zich tot het securitybeleid voor de sectoren waarvoor DGG verantwoordelijk is, te weten spoor, binnenvaart, wegvervoer, zeescheepvaart, havens en ondergrondse pijpleidingen, waarbij als extra dimensie het vervoer van gevaarlijke stoffen op iedere vervoersmodaliteit van DGG van toepassing is.
Hierbij is de maritieme security momenteel prioritair, maar binnen afzienbare tijd zal een verbredingslag plaatsvinden naar de andere vervoersmodaliteiten.

- **DCC**

Bij de Taskforce Security staat de preventie van een terroristische aanval, welke in een ramp kan resulteren, centraal. Indien een ramp niet voorkomen kon worden, komt het DCC in actie. DCC heeft tot taak het verzorgen van de respons van de Bestuurskern van V&W en het Hoofdkantoor van de Waterstaat (HKW) in geval van een crisis.

De basisbezetting van het DCC heeft tot taak:

1. Het opstellen van het algemeen beleidskader voor het crisismanagement van V&W, te accorderen door de Bestuursraad;
2. De voorbereiding van het optreden tijdens een crisis;
3. De algemene procesbewaking tijdens een crisis en de operationele ondersteuning voor beleidsverantwoordelijken van een sector;
4. Het verlenen van nazorg door onder meer het uitvoeren van evaluaties;
5. Het fungeren als kenniscentrum.

Het DCC heeft taken op het terrein van de suppressie van een crisis en heeft in principe geen bemoeienis met het securitybeleid van DGG. Echter, als onderdeel van dit beleid is een uitvoerende taak voor DCC weggelegd, die met name gericht is op berichtenverkeer tussen overheid en het maritieme cluster. Hiervoor worden verbindingen gelegd tussen het DCC en het kustwachtcentrum.

- **DGG**

De DG van DGG heeft als lid van de Bestuursraad van V&W de verantwoordelijkheid voor de ontwikkeling en de in stand houding van een gemeenschappelijke kijk op veiligheid binnen het ministerie. Een bijzonder aandachtspunt vormt daarbij de beveiliging tegen terrorisme. In verband met deze verantwoordelijkheid is een programmadirecteur externe veiligheid aangesteld bij V&W.

Missie en doelen DGG
DGG is verantwoordelijk voor het goederenvervoerbeleid. Dit beleid draagt actief bij aan een veilig, efficiënt en duurzaam goederenvervoersysteem, in het belang van het economisch functioneren en het maatschappelijk welzijn van de Nederlandse samenleving. Het beleid betreft het vervoer over land en over water.

De voor dit onderzoek relevante taken van DGG zijn:
- het ontwerpen en handhaven van wet- en regelgeving;
- het stimuleren van innovaties;
- infrastructuurbeleid en de programmering daarvan voor het DG Rijkswaterstaat en de externe taakorganisaties van V&W;
- het behartigen van Nederlandse goederenvervoerbelangen.

DGG bestaat uit de volgende drie directies:

1. Directie Algemeen Beleid
De directie Algemeen Beleid (A) bevordert verbeteringen in het goederenvervoersysteem als geheel. Ten behoeve van een integraal goederenvervoerbeleid behandelt de directie sectoroverschrijdende vraagstukken, waaronder de ontwikkeling van beleidsvisies. De directie draagt zorg voor de integratie van deze beleidsvisies in kabinetsnota's op het gebied van verkeer en vervoer, leefmilieu en ruimtelijke ordening. Daarnaast vervult zij een coördinerende rol. Zo is de directie verantwoordelijk voor de internationale coördinatie, de coördinatie van bijdragen aan het Meerjarenprogramma Infrastructuur en Transport (MIT) en de coördinatie op het gebied van milieu en Ruimtelijke Ordening (RO).

De voor dit onderzoek relevante taken van de directie A zijn:
- omgevingsverkenning en strategieontwikkeling;
- beleidsontwikkeling m.b.t. Ruimtelijke Ordening (RO), milieu en kennis
- beleidsontwikkeling m.b.t. optimalisatie van vervoersketens (intermodaal vervoer, havens en knooppunten);
- internationaal goederenvervoerbeleid en de beleidsontwikkeling t.a.v de versterking van de positie van Nederland als distributieland.

De directie A kent voor dit onderzoek twee relevante afdelingen en één project die invulling geven aan de kerntaken van de directie. Het gaat daarbij om:
- De afdeling Infrastructuur, Havens en Intermodaal vervoer (IHI).
  Deze afdeling heeft de nationale implementatie van de “International Ship and Portfacility Security Code (ISPS-code)” in de havens op zich genomen;
- De afdeling Algemene Internationale Zaken (AIZ).
  Deze afdeling heeft een coördinerende rol ten aanzien van de verschillende vormen van internationaal beleid, bijvoorbeeld de relatie van Londen met Brussel. Deze relatie komt tot uiting in het feit dat de EU de IMO-regeling ten aanzien van security zal maken tot een Europese verordening. Hiermee wordt op zijn minst bereikt dat er sprake is van een “Level Playing Field” tussen schepenregisters en havens binnen Europa. Tevens geeft dit mogelijkheden tot vereenvoudiging binnen de EU, bijvoorbeeld in de sector short sea;
- Het project Ondergronds Transport/Buisleidingenbeleid.
  Dit project heeft geen directe relatie met het security-beleid van IMO, echter het is wel aangemerkt als vitale infrastructuur en valt dus als zodanig binnen het cluster van externe veiligheid met betrekking tot security. De Taskforce Security DGG heeft vooralsnog geen bemoeienis met ondergronds transport, maar in het kader van de verbreding kan dit veranderen.

2. Directie Transportveiligheid
De directie Transportveiligheid (V) heeft de zorg voor de veiligheid in het goederenvervoer. Deze zorg betreft zowel veiligheidsaspecten van het verkeer en vervoer zélf, als de risico's van

goederenvervoer voor de omgeving (externe veiligheid en milieu). De veiligheidsaspecten van verkeer en vervoer betreffen eisen aan voertuigen, lading en vervoer van gevaarlijke stoffen, uitrusting, personeel, verkeersdeelneming en het gebruik van infrastructuur (o.a. doelgroepstroken, scheepvaartbegeleiding, vaarreglementen). De directie V treedt op als beleidscounterpart van de inspecties op veiligheidsgebied, van het Kustwachtcentrum en van de regionale nautische beheersorganisaties.

De directie V heeft niet het voortouw bij de invulling van het maritieme securitybeleid. Echter, de drie afdelingen herbergen vrijwel alle aspecten van het normale IMO-beleid. Doordat gebruik gemaakt wordt van bestaande regelgeving, is bij de ombouw van deze regelgeving, zowel nationaal als internationaal de inbreng en expertise van deze directie vitaal. Als voorbeeld hierbij: de internationale IMO-regelgeving ten aanzien van het bemannen van schepen[9], welke zowel juridisch als praktisch aangepast en indien nodig uitgebreid moet worden met de opleiding en certificering van zeevarenden als het gaat om security.
Voor dit onderzoek zijn bij directie V drie relevante afdelingen te onderscheiden:

- De afdeling verkeersmanagement (VV).
  Deze afdeling beheert de rijkswateren en de rijkshavenmeesters. De bevoegdheden en verantwoordelijkheden op dit terrein zullen gaan raken aan de ISPS-code, doordat de toegang van schepen in havens in deze ISPS-code geregeld wordt.
- De afdeling vervoermiddelen (VM).
  Deze afdeling staat het dichtst bij de vorming van de internationale regelgeving in IMO-verband op het terrein van veiligheid.
- De afdeling lading en risicobeleid (VL).
  Deze afdeling houdt zich bezig met het vervoer van gevaarlijke stoffen en de daar aan gerelateerde informatiestromen. Deze aspecten van het veiligheidsbeleid zijn van belang bij de behandeling van security-vraagstukken, maar worden in een ander VN-kader dan IMO behandeld.

3. Directie Transport en Infrastructuur

De directie Transport en Infrastructuur (TI) staat voor het bevorderen van goed functionerende vervoersmarkten (weg, binnenvaart, zeescheepvaart en spoor) en het bijbehorende infrastructuur-netwerk in het belang van een efficiënt, veilig en duurzaam goederenvervoersysteem. De directie richt zich met name op transport (de “vervoersmarkt”) en infrastructuur (de “verkeersmarkt”). Bij de vervoersmarkt gaat het onder meer om de marktordening van de aanbieders (wegtransport, binnenvaart, zeescheepvaart, spoor), het bevorderen van de efficiency van de sectoren en het bevorderen van de internationale concurrentiepositie (“Level Playing Field”, markttoegang, etc.). Wat betreft de verkeersmarkt gaat het bijvoorbeeld om de opdrachtgeverrol van het aanbod van vaarweg- en spoorinfrastructuur: verkeersregulerende en benuttingmaatregelen zoals prijsbeleid en inhaal-verboden.

Vooralsnog vinden alleen binnen TZ activiteiten plaats ten aanzien van maritieme security. Naast een belangrijke inbreng in de Taskforce Security DGG ten aanzien van de zeescheepvaart zelf, wordt op deze afdeling ook gewerkt aan de vernieuwing van Conventie 108 van de ILO. Het gaat hier om de “Human Factor”, te weten het gevaar dat uit zou kunnen gaan van subversieve zeelieden. Als voorbeeld hierbij: indien een schip door terroristen als wapen gebruikt kan worden jegens vitale doelen, gaat het dus niet om het schip maar om de intenties van de mensen die aan boord van het schip zijn. Om dit risico te reduceren zal waarschijnlijk eind 2004 een wereldwijde identificatieplicht van zeevarenden en werknemers in de havens van kracht worden. Hiervoor zullen landen die arbeidskrachten leveren voor schepen, moeten overgaan tot de uitgifte van een zogenaamde “Seafarers’ identification-card”, in aanvulling op het paspoort. In het overdrachtsdossier DGG (2003) wordt melding gemaakt van dit gestandaardiseerde identificatiedocument.

Tenslotte is een gecombineerde ILO/IMO-werkgroep opgericht, die zich gaat bezighouden met de security in havens zelf, met name het havenpersoneel. Dit is logisch, want als je de “Human Factor”

[9] Standards of Training, Certification and Watchkeeping (STCW-verdrag)

aan de scheepskant beveiligt, moet je dan ook aan de walkant doen. Dit staat echter nog in de kinderschoenen.

3.5 Beschrijving relevante externe actoren en hun rol bij het securitybeleid van DGG

Het is tegenwoordig gebruikelijk dat beleidsvorming tot stand komt in samenspraak met de externe relaties van de beleidsvormer. DGG vormt hierop geen uitzondering. Hierbij dient opgemerkt te worden dat in het geval van security er sprake is van betrokkenheid van een groot aantal externe actoren, die een rol te vervullen hebben bij de formulering, uitvoering en handhaving van het securitybeleid van DGG. Als voorbeeld hierbij: het voorkomen, dan wel de afhandeling van een security incident in de Rotterdamse haven met een schip berust bij de locale driehoek, bestaande uit politie, brandweer en justitie (met aan het hoofd de burgemeester), waar DGG geen directe zeggenschap over heeft. Om toch de gestelde doelen voor maritieme security te bereiken, is inschakeling van een dergelijke locale driehoek noodzakelijk. De hieronder genoemde externe actoren zijn geïnventariseerd als zijnde van belang voor het maritieme securitybeleid van DGG. Immers, uitvoeringsdiensten en het bedrijfsleven zijn even belangrijke actoren als ministeries.

- **Binnenlandse Zaken en Koninkrijksrelaties**

De minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK), als eerste verantwoordelijke van openbare orde en veiligheid, is een belangrijke actor bij de volgende beleidsdeelterreinen:

1. Reeds eerder genoemde identificatieplicht van zeevarenden
2. De daadwerkelijke bescherming van vitale objecten
3. Een verhoging van de “awareness” (bewustwording en waakzaamheid) op locatie (de Rotterdamse haven).
4. Bij voorkomende incidenten heeft BZK de coördinatie van de afhandeling ervan op landelijk, provinciaal en gemeentelijk niveau. De hieraan ten grondslag liggende bestuurlijke structuur is die van Rijk, provincie en gemeente. Deze structuur wordt benut in de uitvoering van het securitybeleid van DGG.

- **Buitenlandse Zaken**

De minister van Buitenlandse Zaken (BUZA) is verantwoordelijk voor de Buitenlandse Betrekkingen van Nederland. Dit betekent dat dit ministerie een politieke verantwoordelijkheid heeft in de hoogste internationale gremia, waar over security wordt gesproken. Bijvoorbeeld de VN, EU, NAVO en de OESO. Bij voorkomende incidenten heeft dit ministerie een mondiale verantwoordelijkheid voor het welzijn van Nederlandse burgers in het buitenland.

- **Justitie**

De minister van Justitie heeft een eindverantwoordelijkheid op het terrein van wetgeving en speelt ook een rol bij de openbare orde, veiligheid en rechtshandhaving. Het Openbaar Ministerie is een belangrijke partner op lokaal niveau bij de invulling van het locale securitybeleid, zoals bijvoorbeeld in de Rotterdamse haven (locale driehoek: politie, justitie, gemeente). Een voorbeeld van de betrokkenheid van dit ministerie is het feit dat zij draaiboeken beheert op het terrein van de handhaving op de Noordzee. De rol van DGG hierin was, tot 11 september 2001, beperkt tot “search” en “rescue” (het zoeken en redden van drenkelingen op de Noordzee) en bepaalde milieutaken. Security geeft deze taken een extra dimensie die raken aan de bestaande bestuurlijke verhoudingen op de Noordzee.

- **Defensie**

De minister van Defensie heeft een taak in de uitdraging van de Nederlandse politiek in het buitenland: zodra diplomatieke middelen gefaald hebben, resteert nog slechts geweld. Dit begrip moet ruim gezien worden, maar heeft te maken met zowel het handhaven van de vrede als het opleggen van de vrede in gevoelige regio’s van deze wereld. Als voorbeeld hierbij: de vredesmissie in Afghanistan, waarbij militairen van allerlei nationaliteiten, momenteel onder Duits-Nederlands opperbevel, de vrede proberen te handhaven en desnoods op te leggen (“peace-keeping” en “peace-enforcing”). Het

ministerie van Defensie heeft ook een belangrijke taak op de Noordzee. Indien nodig, kan het ministerie van Defensie bijspringen bij de beveiliging van vitale objecten (o.a. die van V&W).

- **VROM**

De minister van VROM heeft de verantwoordelijkheid over nucleaire transporten in Nederland. Indien iemand, al dan niet met kwade bedoelingen, nucleair materiaal transporteert heeft het ministerie van VROM hierin een toezichthoudende rol. Als voorbeeld hierbij: de mogelijkheid dat in een container nucleair materiaal verstopt kan zitten. Indien dit niet is aangemeld bij het ministerie van VROM, zal dit als een potentieel gevaar worden gezien. Hiervoor moeten preventieve maatregelen getroffen worden in de sfeer van de transportsector en de havens. Hiermee is de cirkel met DGG weer rond.

- **SZW**

De minister van SZW is eerste verantwoordelijke in de ILO. Dit VN-orgaan is bezig met de herziening van de identificatieplicht van zeevarenden.

- **AZ**

De minister van AZ is in de huidige situatie, na 11 september 2001, aangewezen als eerste verantwoordelijke voor de voorlichting over security en wat hiermee samenhangt. Tevens heeft het ministerie van AZ een algemeen bekrachtigende rol bij wetgeving over security.

- **IVW**

De Inspectie van V&W (IVW) is belast met de handhaving van de veiligheidswetgeving welke op het terrein van V&W ligt. IVW bestaat uit de divisies vervoer, luchtvaart, rail, scheepvaart en water, maar heeft haar eigen autonome verantwoordelijkheid jegens de minister van V&W en de Tweede Kamer. Echter, binnen de keten van beleidsvorming, implementatie, uitvoering en handhaving is geïntegreerde aanpak noodzakelijk: indien tijdens de beleidsvorming geen rekening gehouden wordt met de uitvoerbaarheid dan wel de handhaafbaarheid is een dergelijk beleid gedoemd tot mislukken.
De Taskforce Security voert overleg met IVW/Divisie Scheepvaart (DS) over de implementatie van Safety Of Lifes At Sea (SOLAS)/ISPS-code aan boord van de schepen en in de havens, welke grosso modo dezelfde methodieken vereisen als de normale veiligheidswetgeving van SOLAS.

- **De Gevolmachtigde Minister van de Nederlandse Antillen**

In het kader van de Koninkrijksrelaties participeert de Gevolmachtigde Minister (GM) in het kabinetsberaad. DGG onderhoudt contacten met het Kabinet van de GM over allerlei koninkrijkszaken die DGG aangaan. Als voorbeeld hierbij: de implementatie en uitvoering van de Schepenwet (SW) en het Schepenbesluit (SB) moet in koninkrijksverband plaatsvinden. Doordat de SW/SB het Nederlandse wettelijke kader wordt voor de inbedding van de internationale regelgeving voor security is hiermee de koninkrijksrelatie beïnvloed op het terrein van security. Dit betekent dat Nederland, in samenspraak met de Nederlandse Antillen, een gezamenlijk wettelijk kader schept. Dit geldt alleen voor de zeescheepvaart. Hoe binnen de koninkrijksrelatie omgegaan moet worden met de havens is momenteel nog niet bekend. Waarschijnlijk hebben de Nederlandse Antillen hierin een eigen verantwoordelijkheid, omdat er geen koninkrijkswetgeving over havens bestaat.

Een en ander mondt uit in een verzoek tot bijstand van de Nederlandse Antillen aan Nederland. DGG zal waarschijnlijk op zijn minst steun moeten verlenen in de sfeer van technische ondersteuning en de opbouw van expertise aan en in de Nederlandse Antillen.

- **Koninklijke Vereniging van Nederlandse Reders**

Zeescheepvaart is al eeuwenlang gezichtsbepalend voor Nederland. Zowel op maatschappelijk, sociaal als economisch gebied is de zeescheepvaart diep verankerd in de Nederlandse samenleving. De maritieme sector zorgt dan ook voor een substantiële bijdrage aan de nationale economie.
Ter behartiging van de belangen van de in Nederland gevestigde rederijen in de meest ruime zin is de KVNR opgericht.
De vereniging zet zich in voor de collectieve en individuele belangen van ondernemingen in deze sector. De collectieve belangenbehartiging is gericht op het instandhouden en verbeteren van een

internationaal concurrerend ondernemingsklimaat op economisch en sociaal gebied. De KVNR biedt een neutraal platform om de redersbelangen van zowel grote als kleine bedrijven op verschillende gebieden en op verschillende niveaus te behartigen.
Om deze functie effectief uit te kunnen voeren, onderhoudt de vereniging contacten met de Nederlandse overheid en instanties die zich met maritieme zaken bezighouden. Deze contacten betreffen zowel beleid als uitvoering. De vereniging houdt zich ook actief bezig met de internationale scheepvaartontwikkelingen. Daarvoor zijn er contacten met intergouvernementele organisaties en internationale redersverenigingen.

De individuele dienstverlening is een belangrijk onderdeel van de activiteiten van de KVNR. Het bureau van de KVNR dient als vraagbaak voor uiteenlopende onderwerpen. Daartoe worden de nationale en internationale ontwikkelingen op het gebied van wet- en regelgeving nauwkeurig gevolgd. Relevante zaken worden aan de leden doorgegeven. Indien een situatie daar aanleiding toe geeft, zal de vereniging de zaken bij de juiste instanties aanhangig maken en pleiten voor een geschikte oplossing.
De belangenbehartiging beperkt zich niet tot reders die schepen onder Nederlandse vlag exploiteren. Door de actieve participatie van de KVNR in diverse internationale organisaties, heeft het lidmaatschap ook meerwaarde voor reders met schepen die onder vreemde vlag varen. De KVNR meldt in haar jaarverslag (2001) wat haar taken zijn.

Ten gevolge van het feit dat meer dan 90% van de Nederlandse reders lid of geassocieerd lid van de KVNR is, beschouwt DGG de KVNR als representatieve vertegenwoordiging van het bedrijfsleven en beschouwt haar dus als serieuze gesprekspartner.
Zoals reeds beschreven is het bij DGG goede gewoonte haar doelgroep te laten meepraten over beleidsdoelstellingen en formulering van beleid om tot een verantwoorde afweging van de belangen te kunnen komen.
Dit uit zich in het geval van maritieme security op diverse wijzen:

1. Daadwerkelijke participatie in het overleg in IMO-verband als lid van de Nederlandse delegatie.
2. Meepraten over te formuleren standpunten in internationaal overleg tijdens de voorbesprekingen.
3. Informele contacten (netwerken).
4. Participatie in de nationale follow-up: implementatie van securitybeleid.

ad. 1: Tijdens de internationale vergaderingen van de IMO heeft de vertegenwoordiging van de KVNR een actieve ad-hoc inbreng voor ter plekke te nemen besluiten, die nog niet voorbereid konden worden en waardoor het brede standpunt dus niet gehoord kon worden. Deze rol kan versterkt worden door de internationale organisatie van de reders “the International Chamber of Shipping (ICS)” en vele daaraan verwante deelorganisaties zoals bijvoorbeeld Intertanko, die de belangen van reders met tankschepen behartigt. Aldus is het mogelijk om een mondiale redersinbreng te hebben. De delegatieleiding (overheid, in de vorm van DGG) kan vervolgens een objectieve belangenafweging maken die nog verder reikt dan de nationale afweging. Afstemming in EU-verband vindt eveneens ter plekke plaats.

ad. 2: Het is gebruikelijk dat een brede maatschappelijke discussie gevoerd wordt om tot het voorbereiden van Nederlandse standpunten te komen (al dan niet EU-breed). Gedurende de formulering van de internationale regelgeving (2002) heeft dit proces voortdurend plaatsgevonden.

ad. 3: Het is vaak nodig om bepaalde zaken in kleiner verband dan wel individueler te behandelen, waarvoor DGG “de boer opgaat”. Met andere woorden: DGG spreekt ook met individuele reders, omdat er diversiteit is in marktbenadering.

ad. 4: Als gevolg van de tendens om verantwoordelijkheden bij de markt te leggen, zal implementatie en uitvoering van de internationale regelgeving voor een niet onbelangrijk deel bij het bedrijfsleven gelegd worden. Dit betekent dat DGG zich moet beraden over de vraag of en in hoeverre hierop nog toezicht nodig is. Deze vraag krijgt een extra dimensie ten gevolge van het feit dat het hier om zaken

gaat die met de staatsveiligheid te maken hebben. De bestuurlijke afweging van het op afstand plaatsen van overheidstaken krijgt een extra dimensie.

Een voorbeeld van het op afstand plaatsen van overheidsverantwoordelijkheden is het "International Safety Management (ISM)"-systeem, waarbij de reder voor een zeer aanzienlijk deel zelf instaat voor de veiligheid van zijn bedrijfsvoering (inclusief de schepen) met de overheid in een toezichthoudende rol. Dit is de moderne interpretatie van handhaving. De ISPS-code kan gezien worden als een soortgelijke "Code of Conduct" c.q. "best-practises systeem": de zelfwerkzaamheid van de markt, afgezet tegen het staatsbelang. De discussie hoe hier invulling aan te geven, gegeven het zwaardere belang van de staatsveiligheid (een dimensie in marktwerking), is nog niet afgerond.

Samengevat: kan en mag de overheid een algemeen maatschappelijk belang overlaten aan het bedrijfsleven, dat andere belangen nastreeft? Ethisch gezien is het denkbaar, indien het resultaat in het oog gehouden wordt, wat bereikt kan worden door adequaat toezicht.

- **Nationale Havenraad**

De NHR is het overlegorgaan van de Nederlandse zeehavens, de Rijksoverheid en de belangenorganisaties van het bedrijfsleven in de havensector. De NHR is een publiekrechtelijk orgaan dat formeel onder DGG valt. De NHR brengt gevraagd en ongevraagd adviezen uit over onderwerpen die van belang zijn voor de Nederlandse zeehavens. Voorts kan de NHR door de leden worden ingeschakeld bij gemeenschappelijke projecten. Tot de taken van de Raad behoort tevens het bevorderen van de samenwerking tussen de partijen die bij zeehavenaangelegenheden betrokken zijn. De NHR is opgericht bij Koninklijk Besluit van 7 mei 1986. De NHR bestaat uit een onafhankelijk voorzitter en 23 leden.

De betrokkenheid van de NHR bij het maritieme securitybeleid van DGG is pas recentelijk door deze raad erkend. Dit komt omdat zij zichzelf als een adviesorgaan voor de minister van V&W zien. Echter, de NHR is een overlegplatform waar belanghebbenden rond één tafel zitten, wat mogelijkheden geeft om te komen tot een landelijke aanpak van de implementatie van de ISPS-code.

- **Havenautoriteiten**

Naast de schepen maakt de ISPS-code gewag van zogenaamde "port-facilities" waar een soortgelijk "security management" systeem van "best-practises" gerealiseerd moet worden. Hierbij spelen de havenautoriteiten en het bedrijfsleven van dertien daarvoor in aanmerking komende Nederlandse havens een vitale rol: via hen moet de verbinding gelegd worden naar de bedrijven die - analoog aan de reders - het nieuwe security-regime moeten realiseren.

Een belangrijke speler hierbij is het Haven Bedrijf Rotterdam (HBR), dat zelf al initiatieven heeft ontwikkeld om een security-regime in de Rotterdamse haven in te voeren. Op 1 januari 2004 is de publiekrechtelijke status van het HBR gewijzigd naar dat van een semi-overheidsorganisatie (ZBO). Samen met deze verandering in publiekrechtelijke status is de naam Gemeentelijk Havenbedrijf Rotterdam (GHR) gewijzigd in het huidige HBR. Dit plaatst de haven van Rotterdam beter op de internationale kaart. De bij de KVNR blootgelegde afweging ten aanzien van de bewaking van een maatschappelijk belang door private ondernemingen begint hier ook een rol te spelen.

Het HBR beheert namens de gemeente Rotterdam het bijna 11.000 hectare tellende Rotterdamse haven- en industriecomplex. Dit gebied heeft verschillende belangrijke functies: het is een verzamelplaats voor internationale goederenstromen, herbergt industriële clusters en logistieke dienstverleners en fungeert als "draaitafel" voor internationale productienetwerken. Het haven- en industriecomplex is een belangrijke dynamo voor zowel de nationale als de internationale economie.

Vanouds kent het HBR de volgende twee taken:
1. Het ontwikkelen, construeren, managen en opereren van het haven- en industriecomplex;
2. Het effectief, veilig en efficiënt afhandelen van scheepsverkeer.

Van havens wordt echter steeds meer verwacht wat overslag, industrie en distributie en andere diensten aangaat. Onze economie is aan het globaliseren en activiteiten worden overal ter wereld uitgevoerd. Dit leidt tot een opwaardering en toename van transport, waarin de haven van Rotterdam slechts een link is in logistieke en industriële netwerken. Daarom is het HBR niet alleen actief in de haven zelf, maar ook daarbuiten.
Elke vier jaar publiceert het HBR een business plan, waarin de organisatie aangeeft hoe het haar rol verder wil ontwikkelen en welke aspecten specifieke nadruk en prioriteit zullen krijgen gedurende die periode.

Het HBR hanteert de volgende missie:
"Het versterken van de positie van het Rotterdamse haven- en industriecomplex in Europees perspectief. Nu en op de lange termijn." Hiervoor positioneert het HBR zichzelf als havenautoriteit en internationale dienstverlener.

Het HBR:
- Ziet in de haven toe op de basisvoorwaarden wat betreft orde, veiligheid en toegankelijkheid;
- Faciliteert in toenemende mate economische bedrijvigheid in het haven- en industriecomplex;
- Versterkt de logistieke en industriële netwerken en clusters waar Rotterdam deel van uit maakt;
- Investeert in een duurzame woon- en werkomgeving;
- Maximaliseert haar one-stop-shop concept door zowel bestaande als potentiële nieuwe klanten te voorzien van alle relevante informatie over vergunningen, infrastructuur, het milieu en gespecialiseerde marktkennis. Ze hoeven slechts contact op te nemen met één partij: het HBR.

Analoog aan de beschrijving van de hierboven vermelde KVNR, moesten de havens betrokken worden bij de beleidsvorming en de uitvoering van de internationale regelgeving. Hierbij deed zich het probleem voor dat kleinere havens de voortrekkersrol van Rotterdam plachten te interpreteren als een middel om haar (politieke) invloed te vergroten. Inmiddels is het vertrouwen uitgesproken in Rotterdam als vertegenwoordiger van de Nederlandse havens in internationale beleidsvorming en regelgeving. De NHR heeft hierin een belangrijke rol gespeeld.

De voordelen van de voortrekkersrol van het HBR voor de Nederlandse overheid (DGG) zijn tweeledig:
1. Er kan een landelijke beleidsafstemming plaatsvinden.
2. Het schept mogelijkheden tot een landelijke uniforme implementatie van het maritieme securitybeleid (met ruimte voor de individuele omstandigheden).

Ten aanzien van punt twee kan gemeld worden dat de Rotterdamse aanpak in grote lijnen door de andere Nederlandse havens geadopteerd zal worden. Dit kan voor DGG als succes worden aangemerkt in bestuurlijke zin, omdat een uniforme bestuurlijke aanpak de beheersbaarheid bevordert. Dit is nodig omdat Nederland als "contracting government" garant moet staan voor de kwaliteit en de geloofwaardigheid van de Nederlandse uitvoering van de internationale regelgeving, mondiaal gezien.

De discussies over de vraag hoe het implementatietraject er uit ziet worden bemoeilijkt door het feit dat er geen geschikt juridisch kader aanwezig is voor havens, zoals we dat hebben kunnen zien bij de scheepvaart (SW/SB). In tegenstelling tot wat voor de scheepvaart geldt is betrokkenheid van andere ministeries op dit gebied een absolute vereiste.

De wijze waarop de ISPS-code/EU-verordening in Nederland geïmplementeerd zal worden, staat nog volop ter discussie. De gekozen conceptuele benadering is van rechtstreekse invloed op de te formuleren nationale wetgeving. De wetgevingsjuristen zullen immers eerst moeten weten waarover zij praten voordat zij dit kunnen omzetten in een wet. Het belang van de havenbedrijven is gelegen in het feit dat zij een zeer belangrijke rol te vervullen hebben om de implementatie van de ISPS-code in hun eigen haven te realiseren. Dit staat los van de vraag in hoeverre zij er garant voor moeten staan, omdat de Rijksoverheid, oftewel de "contracting government", formeel garant staat jegens het internationale SOLAS-verdrag.

De ISPS-code bestrijkt slechts zogenaamde “port facilities”, maar niet de haven als geheel. De tendens is echter dat zonder een “port security plan” een “port facility security plan” niet goed uitvoerbaar is.

3.6 IMO

IMO houdt zich bezig met internationale regelgeving jegens de zeescheepvaart, met name ten aanzien van veiligheid en milieu. Hiervoor zijn diverse conventies/verdragen afgesloten, die hun beslag hebben gekregen in internationale regelgeving. Twee voorbeelden van een dergelijke conventie zijn:

1. Maritime Pollution (MARPOL)-conventie: gericht op het voorkomen van vervuiling op zee en van de lucht;
2. SOLAS: gericht op de veiligheid van de zeescheepvaart in de meest brede zin, wat varieert van technische veiligheid (oftewel interne veiligheid) tot “International Safety Management” (ISM), wat als externe veiligheid te betitelen is. SOLAS is van oorsprong een veiligheidsconventie. Deze veiligheidsconventie wordt nu aangewend als platform voor internationale regelgeving op het terrein van security. Dit is terug te vinden in technische uitrustingshoofdstukken en de creatie van een nieuw IMO security-hoofdstuk, te weten Chapter 11-1/2. Dit securityhoofdstuk vormt het kader van waaruit regelgeving wordt opgesteld. Voor het securitybeleid betekent dit dat deze regels leiden tot de zogeheten ISPS-code. In dit kader is het relevant te vermelden dat, hoewel SOLAS in principe alleen gericht is op schepen, de ISPS-code ook delen van havens bestrijkt.

Alhoewel de ISPS-code in principe gereed is, zullen nog enige verfijningen plaatsvinden. Waar het om gaat is dat deze Code een internationaal geaccepteerde verzameling van “best-practises” is, en als zodanig fungeert als internationale standaard.

Hoewel in dit kader de stand van zaken niet wordt behandeld, moet toch worden opgemerkt dat vertragingen die optreden bij de implementatie van de regelgeving aanleiding zijn geweest om organisatorische maatregelen te treffen die moeten uitmonden in een hulpprogramma en een IMO securityfonds. De belangrijkste aanleidingen hiervoor waren:

1. Er is een groot verschil in expertise tussen ontwikkelde en minder ontwikkelde landen;
2. Het kosten-baten aspect speelt een grote rol: het mag niet zo zijn dat onzinnige investeringen in security plaatsvinden, die een minimaal resultaat opleveren;
3. Sociale culturen in landen verschillen: het ene land zal gewetensvoller met de nieuwe uitdagingen omgaan dan het andere land: het is momenteel nog niet te overzien hoe bezoekende schepen in bepaalde landen behandeld zullen worden, het is denkbaar dat op grond van de bevoegdheden van de Code oneigenlijke maatregelen genomen worden;
4. Het ene land is economisch beter in staat aan de eisen te voldoen dan het andere land.

Op 13 december 2002 vond een diplomatieke conferentie plaats waarin het fundament voor een nieuw security regime voor de maritieme sector (havens en zeescheepvaart) werd gelegd. Tijdens deze conferentie is overeenstemming bereikt over het invoeren van internationale regelgeving op het gebied van maritieme security. Het gaat daarbij om een reeds bestaand IMO verdrag, namelijk het “International Convention for the Safety of Life at Sea”, dat uitgebreid is met de nieuwe ISPS-code. Het verdrag is door 102 landen getekend.

De nieuwe ISPS-code wordt automatisch van kracht per 1 juli 2004 (gevolg van de koppeling aan SOLAS-verdrag), omdat geen voldoende meerderheid tegen het verdrag is opgestaan per 31 december 2003. De hierbij gehanteerde minima zijn: 30% van de lidstaten óf 50% van de wereldtonnage van de schepen.

Enkele belangrijke aspecten van de ISPS-code:

- Reders en schepen: schepen moeten over een goedgekeurd “ship security plan“ beschikken, er dienen voor security verantwoordelijke, getrainde “ship and company security officers” te zijn, gedetailleerde informatie over geschiedenis en eigendom van het schip dient aanwezig te zijn en schepen moeten een zichtbaar registratienummer op de romp krijgen. Tevens moeten bepaalde voorzieningen aan boord van het schip getroffen worden, zoals een alarmeringssysteem en fysieke toegangscontrole;
- Havens en port facilities: in analogie met het bovenstaande worden goedgekeurde “port facility security plans” vereist;
- Overheidsverantwoordelijkheden: handhaving en toezicht op de uitvoering van het nationale security-beleid, zoals gevoerd op de Nederlandse vloot en in Nederlandse havens, waaronder certificering, vergunningen, het uitvoeren van risk-assessment per schip of per haven-faciliteit en het reeds genoemde wettelijk kader.

3.7 Taskforce Security van DGG

Om invulling te geven aan de internationale regelgeving - voortvloeiend uit de ISPS-code - heeft de DG van DGG besloten per 1 december 2002 de Taskforce Security in te stellen die zorg moet dragen voor de voorbereiding en uitvoering - in nationaal en internationaal verband - van het V&W security beleid ten aanzien van het goederenvervoer. De Taskforce Security is DGG-breed opgezet. Primair richt deze Taskforce zich op de security van het maritieme cluster. Het maritieme cluster omvat zeescheepvaart en havens. Als gevolg van eventuele introductie van een haven- en ketenrichtlijn door de EU, is het denkbaar dat de Taskforce Security zich in de toekomst hiermee gaat bezighouden. Dit valt precies binnen het werkterrein van DGG, namelijk de vervoersectoren. In het informatiedossier DGG (2003) staat beschreven dat DGG een samenhangend security beleid vaststelt voor alle V&W-terreinen en hoe dit beleid ten uitvoer moet worden gebracht.

Onder de opdracht aan de Taskforce Security vallen o.a. de volgende taken:

1. Het verder ontwikkelen van een V&W securitybeleid ten aanzien van het goederenvervoer (beleidskader) waarbinnen geopereerd wordt. Meer concreet betekent dit: het maken van wetten & regelgeving. Onderdelen hiervan zijn:
   - Maatregelen treffen ter minimalisering van het risico op mogelijke aanslagen (voorkomen kan helaas niet);
   - Het waarborgen van een zgn. “Level Playing Field” met andere landen. In een notendop betekent dit het waarborgen van gelijke concurrentieverhoudingen tussen landen.
2. Fungeren als aanspreekpunt voor security voor DGG en buitenwereld (ambtelijk/bedrijfsleven);
3. Zorgdragen voor interne DGG/V&W en externe coördinatie. Met andere departementen (BZK, Justitie, Financiën) afbakenen wie verantwoordelijk is voor welke aspecten. Vervolgens moet dit in de Tweede Kamer worden neergelegd. Als voorbeeld hierbij de militaire transporten door Nederland naar aanleiding van de crisis met Irak. Na de gebeurtenissen van 11 september 2001 is het nog steeds niet duidelijk welk departement en welk organisatieonderdeel van V&W waarvoor verantwoordelijk is. Dit resulteert in het volgende punt.
4. Expliciteren DGG/V&W verantwoordelijkheden en bevoegdheden. Zo is inmiddels gebleken dat in het kader van openbare orde en veiligheid ten aanzien van militaire transporten, V&W bijna geen verantwoordelijkheden en bevoegdheden heeft.
5. Onderhouden van nationale en internationale relaties: bilateraal, EU, IMO, Conference Européenne des Ministres des Transports (CEMT), Organisatie voor Economische Samenwerking en Ontwikkeling (OESO);
6. Uitwerken van een voorstel voor toekomstige inbedding van security binnen DGG: de organisatie is nog niet structureel berekend op security-vraagstukken. In het geval van crisisbeheersing en rampenbestrijding is dit wél het geval, waar crisisbeheersing onderdeel van het normale beleid is geworden.

Voorlopig heeft de DG besloten om de Taskforce Security niet onder te brengen bij één van de directies, maar deze rechtstreeks onder de eindverantwoordelijkheid van de plaatsvervangend DG te laten vallen. In geval van afwezigheid van de plv. DG, is de DG zelf eindverantwoordelijke. De Taskforce Security zal nauw samenwerken met de V&W brede projectdirecteur.

Gedurende de periode van 1 december 2002 tot op heden is een afdelingshoofd van directie Algemeen Beleid, die deel uitmaakt van DGG, grotendeels vrijgesteld van diens huidige taken. Deze persoon fungeert als leidinggevende van de Taskforce Security en is procesmatig en inhoudelijk het eerste aanspreekpunt. De DG heeft bewust geen einddatum gekozen omdat naar verwachting in de periode die hieraan voorafgaat duidelijk zal worden wat er nationaal en internationaal op DGG afkomt en wat de DGG verantwoordelijkheden (ook voor de langere termijn) zijn. Ten gevolge van bestuurlijke en organisatorische veranderingen binnen V&W, is de rol van de Taskforce Security in de toekomst nog niet helder.

De plaatsvervangende leidinggevende van de Taskforce Security is een ambtenaar van TZ. Deze persoon is inhoudelijk het eerste aanspreekpunt binnen de Taskforce Security. Binnen DGG zijn momenteel drie ambtenaren parttime aangesteld als uitvoerende beleidsmedewerkers. Interne betrokkenheid is er ook van V en IVW. De juridische inbreng, het verzorgen van het wettelijk kader, zal geschieden door de Hoofddirectie Juridische Zaken (HDJZ).

De Taskforce Security bedient zich van diverse werkgroepen om de implementatie van het beleid mogelijk te maken:

1. Werkgroep Schepen en Reders: een op initiatief van de reders tot stand gekomen samenwerkingsverband tussen het bedrijfsleven en de overheid;
2. Werkgroep Havens: een samenwerkingsverband tussen regionale en landelijke overheden, gericht op de havens;
3. Werkgroep “Securidee”: een samenwerkingsverband tussen beleid en uitvoering van DGG en IVW/DS;
4. Werkgroep Wetgeving: deze werkgroep realiseert het totale wetgevingstraject;

Daarnaast functioneert een werkgroep die zich bezighoudt met de identiteitsproblematiek van zeevarenden en eventueel havenpersoneel. Deze werkgroep valt formeel niet onder de Taskforce Security.

3.8 Plan van aanpak “Maritieme Security”

3.8.1 Algemeen

Inmiddels is het besluitvormingsproces in IMO-verband voltooid, waarmee nu het moment aanbreekt om hier nationaal invulling aan te geven. De materie is zeer veelzijdig, en bestrijkt diverse disciplines en andere instanties. Binnen V&W zal het forse extra inspanningen vergen van DGG, HDJZ en IVW.

Het plan van aanpak “Maritieme Security” richt zich op de volgende aspecten van implementatie en uitvoering:

1. Schepen en reders: deze hebben een eigen verantwoordelijkheid om security-plannen op te stellen, security-assessments uit te voeren en security-functionarissen aan te stellen. Hieraan is dan een certificeringsproces van de zijde van de overheid gekoppeld, analoog aan de veiligheidswetgeving voor de zeescheepvaart.
2. Havens en havenfaciliteiten: ook havenfaciliteiten moeten security-plannen opstellen, security-assessements uitvoeren en security-functionarissen aanstellen. De vraag of dit gekoppeld moet worden aan een vergunningenstelsel, moet nog beantwoord worden. Een security-plan van een havenfaciliteit moet ingepast worden in de security-plannen van een haven in haar totaliteit, wat tot de verantwoordelijkheid van de desbetreffende gemeente behoort, en wat niet onder de ISPS-code valt.

3. Het scheppen van een wettelijk kader, met eventueel gebruikmaken van bestaande wetgeving. Hierbij doet zich het probleem voor dat de bestaande wetgeving niet bedoeld was voor security, wat wellicht een speciale security-wet nodig maakt. Tevens hebben gemeenten hun eigen autonomie op het terrein van openbare orde en veiligheid: V&W heeft hier geen zeggenschap over. Er zal dus een manier gevonden moeten worden om de IMO-regelgeving op te nemen in de bevoegdheden van de burgemeester.
4. Handhaving en controle: voor de schepen die onder Nederlandse vlag varen, is het normale toezicht- en handhavingscontrolemodel van toepassing: de daadwerkelijke controles aan boord van de schepen worden uitgevoerd door zogenaamde "recognized security organisations". Deze worden op hun beurt door de Nederlandse overheid gecontroleerd en aangestuurd middels een contract. Voor schepen die onder buitenlandse vlag varen en Nederlandse havens bezoeken (ongeveer 40.000 schepen op jaarbasis), wordt met behulp van een "targeting" systeem[10] een keuze gemaakt of het schip zich aan de regels houdt. Indien dit niet het geval blijkt te zijn kunnen extra, restrictieve maatregelen worden genomen. Deze kunnen heel ver gaan, tot het uitwijzen van het schip toe.[11]
   De havenfaciliteiten worden eveneens gecertificeerd zodra zij aan de eisen voldoen. Alhoewel nog niet met zekerheid bekend is, zal de IVW/DS hoogstwaarschijnlijk in de toekomst de handhaving (controle op een duurzaam voldoen aan de regels) op zich nemen. Dit gaat pas spelen ná 1 juli 2004, en heeft niet de hoogste prioriteit.
5. Expertise en opleidingen: het is nog onbekend hoe dit ingevuld moet worden. De kennis van security moet opgebouwd worden, en op grond van de ISPS-code zal een opleidingsprogramma uitgewerkt moeten worden, compleet met certificering.
6. Ontwikkeling van een identiteitskaart voor zeevarenden en personen, werkzaam in de haven. Hiervoor zou aanpassing van de paspoortwet nodig zijn. Of dit de juiste juridische richting is, moet nog vastgesteld worden.

3.8.2 De situatie in Nederland

Doordat de focus van security momenteel gericht is op (maritiem) transport en infrastructuur is V&W een belangrijke actor op deze terreinen. De (politieke) magnitude van de dossiers is van dien aard dat de impact op de samenleving groot is. Een goed voorbeeld is de door de Amerikanen afgekondigde eis dat minimaal 24 uur voor aanvang van een reis naar de VS de ladingdocumentatie in het bezit moet zijn van de VS (Besier, 2002: 5). Ondanks aanvankelijke bezwaren en protesten is inmiddels gebleken dat het bedrijfsleven hier aan kan voldoen en komt men tot de ontdekking dat deze manier van werken kwaliteitsverbeterend werkt.
Inmiddels is het bedrijfsleven (zowel de reders als de havenfaciliteiten) ver op weg om aan de regels te voldoen zoals die door de EU en de IMO zijn opgelegd. Op basis van "toolkits" – al dan niet elektronisch – kan een afweging worden gemaakt welk risico er gelopen wordt. Dit dient als uitgangspunt om tot een beschrijving van procedures en veiligheidsmaatregelen te komen (het "ship-security plan" en het "port-facility security plan"). Goedkeuring van deze plannen, gevolgd door de verificatie van de implementatie aan boord dan wel in de port facility levert "compliance" op.[12]

De betrokkenheid van andere ministeries bij security-beleid wordt hier onder vermeld en komt op de volgende wijze tot uiting:

- BZK: vitale infrastructuur en processen, beveiliging, AIVD, NAVO, KLPD. Openbare orde en veiligheid, positie en rol burgemeesters, en op de achtergrond ook de provincies;
- BUZA: algemeen politiek, mondiaal, belangenbehartiging in met name de VS;

[10] Targeting is op basis van relevante informatie over het schip beslissen of het desbetreffende schip in aanmerking komt voor extra, hernieuwde controles.
[11] Bij targeting en eventuele restrictieve maatregelen zijn de positie van de burgemeester, zijn bestuurlijke rol ten aanzien van de openbare orde en veiligheid, gevoegd bij de inlichtingenpositie (AIVD en andere bronnen, waaronder maritieme) van het grootste belang. Een besluit tot verregaande maatregelen, zoals het verhogen van het security-level in een haven, wordt in principe genomen door de bestuurlijke driehoek: de ministers van AZ, BZK en Justitie.
[12] "Compliance" wil zeggen dat betrokkenen aan de regelgeving voldoen en *blijven* voldoen.

- Justitie: toelatingsbeleid, identiteit van zeevarenden en anderen die bij het maritieme cluster betrokken zijn (dit laatste geldt ook voor BZK);
- SZW: identiteit, ILO;
- Financiën: douane, documentatie.

3.8.3 De strategie van DGG

Nederland is voorstander van uniforme, internationale regelgeving omdat daardoor de kans op willekeur ten opzichte van onze schepen in buitenlandse havens verkleint, en de internationale concurrentiepositie van onze reders en de regionale concurrentiepositie van onze havens het beste gewaarborgd wordt. Een "Level Playing Field" is daarbij het uitgangspunt voor de Nederlandse positie.

Een ander uitgangspunt is dat de diverse maatregelen een redelijke kosten/baten verhouding in zich hebben. Deze (algemene) opstelling wordt gedeeld door de KVNR en de Nederlandse havenautoriteiten. Internationale regelgeving is meestal een redelijk haalbaar gemiddelde (compromis) van standpunten. Het gevaar van unilaterale maatregelen wordt hierdoor ook verminderd.

De Nederlandse positie in Europa is bereikt door de introductie van EU-regelgeving: het "Level Playing Field" binnen Europa wordt het beste door een verordening gewaarborgd. Inmiddels heeft de "European Maritime Safety and Security Authority (EMSSA)" bevoegdheden gekregen de landen hier op aan te spreken en te controleren.[13]
Gebaseerd op ervaringen in het verleden zal DGG bilaterale overeenkomsten zoals die tussen het ministerie van Financiën en US Customs vermijden, tenzij deze de instemming van Brussel hebben. Bij de afsluiting van de overeenkomst tussen de douanes van Nederland en de VS in Rotterdam is DGG niet betrokken geweest. Echter, bij monde van DG TREN[14] is DGG geconfronteerd met het feit dat dergelijke overeenkomsten niet de instemming van Brussel hebben.

Daarnaast mag de verhouding met de Amerikanen, die gedurende dit jaar is opgebouwd, en die thans uitmondt in gezamenlijk regulier overleg tussen DGG en functionarissen van de Amerikaanse ambassade, niet te lijden hebben van de restricties welke vanuit de EU worden opgelegd. Uitgangspunt hierbij is dat deze verhouding haar nut kan hebben voor zowel de Nederlandse vloot als voor de Nederlandse havens: het soepel verlopen van wederzijdse betrekkingen is een regelrecht voordeel dat niet verloren mag gaan. Zodra sprake is van het sluiten van overeenkomsten moet hiermee als gevolg van de Europese factor met terughoudendheid worden omgegaan, maar vanuit een positieve grondhouding. Het is derhalve zaak met de VS te blijven communiceren. Inmiddels zijn als proefproject op bepaalde plaatsen in de havens van Rotterdam nucleaire detectiepoorten geplaatst.

Handhaving van het "Level Playing Field", voor zowel de schepen als de havens is een belangrijk uitgangspunt. De nieuwe SOLAS-toevoeging en de Code bevatten nuttige aanknopingspunten in de sfeer van controles, maar gaan hierin niet echt ver. Het mechanisme is analoog aan dat van Port State Control[15]. Ook zijn rapportagemechanismen voorzien. De opstelling van Nederland wordt derhalve bepaald door de effectiviteit van het security regime. Nederland behoudt zich hierbij het recht voor om hogere standaards te hanteren, en ziet het IMO-niveau als een minimum. In de nationale voorbereidingen voor de implementatie wordt uitgegaan van de IMO standaard.

Nederland zal zich bilateraal moeten verstaan met haar buurlanden. Eventuele bilaterale overeenkomsten zullen in Brussel kenbaar gemaakt moeten worden. Tevens moet Nederland zich voorbereiden op te formuleren EU standpunten op diverse terreinen van security nadat de overeenkomst in Londen getekend is.

---

[13] Observatie: mondiaal is een dergelijk mechanisme veel minder hard.
[14] Dit is het Europese Directoraat-Generaal voor Transport en Energie.
[15] Bij Port State Control is de havenstaat bevoegd schepen te inspecteren en in het uiterste geval aan de ketting te leggen.

Het bedrijfsleven is een belangrijke schakel in de securityketen, én in het nieuwe security regime van de IMO, maar heeft hierin haar eigen verantwoordelijkheid. Afgezien van een stimulerend beleid gedurende de nationale implementatiefase zal de sector in belangrijke mate haar eigen verantwoordelijkheden moeten dragen, analoog aan de handhaving op het terrein van veiligheid zelf.

Kort samengevat: Nederland conformeert zich aan het (mondiale) streven om tot een veiliger scheepvaartsector te komen, met als uitgangspunt het handhaven van "Level Playing Field" en een redelijke kosten/baten verhouding.

DGG heeft géén bestuursverantwoordelijkheden voor de infrastructuur, maar in transport- en logistieke processen is sprake van een duidelijke verantwoordelijkheid voor nationale en internationale beleidsvorming, zoals in IMO en EU. Deze uit zich momenteel in de maritieme sector, maar zal later waarschijnlijk eveneens de andere sectoren gaan bestrijken.

Enige observaties van de Taskforce Security

1. Thans heeft DGG verantwoording voor het functioneren van de Rijkshavenmeesters in de havens, terwijl de verantwoordelijkheid van openbare orde en veiligheid bij de burgemeester berust. Ten gevolge van de EU/IMO-regelgeving neemt de beleidsverantwoordelijkheid van DGG toe, met name op het terrein van "port security"[16], met inachtneming van de positie van de burgemeester op het terrein van openbare orde en veiligheid. Dit laatste moet ingebed worden in het nieuwe security regime.
2. DGG heeft de verantwoording voor de beleidsvorming inzake het totale EU/IMO-pakket, maar moet hierbij rekening houden met de verantwoordelijkheden en bevoegdheden van andere ministeries en onder hen ressorterende instanties.
3. De nieuwheid van de materie, gevoegd bij het brede terrein van bevoegdheden en verantwoordelijkheden dat bestreken moet worden vergt een zware coördinatiestructuur, ook in de toekomst.
4. Gegeven de implementatietijd en het politieke gewicht van security is er sprake van een gerichte, projectmatige aanpak met een zwaar projectleiderschap.

Doordat het security-beleidsterrein inmiddels een behoorlijke vlucht genomen heeft, wordt thans nagedacht over versterking, opschaling en verbreding van de structuur van verantwoordelijkheden en hoe hier mee om te gaan.

3.8.4 Sturing/regie

Het geheel van inspanningen wordt aangestuurd om de processen richting te geven en om besluiten te nemen. Het instrument dat hiervoor gebruikt wordt, is de Taskforce Security.

Er is voor advisering, consultatie en besluitvorming een "expertgroep" opgericht, die – alhoewel zij geen officiële status heeft – fungeert als stuurgroep voor de minister. De plaatsvervangend DG van DGG fungeert hierbij als voorzitter.

Tevens is voor brede consultatie en overleg de Nationale Commissie Beveiliging Zeescheepvaart en Havens (NCBZH) opnieuw tot leven gebracht. Hierin hebben diverse vertegenwoordigers van het maritieme cluster en de overheid zitting. Er komen voornamelijk praktische zaken aan de orde. De projectleider van de Taskforce Security fungeert hierbij als voorzitter.

[16] De havenbeveiligingswet (HBW) valt onder de zogenaamde Tijdelijke referendumwet (Trw). Dit impliceert dat de wet niet in werking getreden is op de dag na uitgifte van het Staatsblad waarin ze gepubliceerd is, zoals in de wet staat, maar pas enige weken na de publicatie in werking zal treden. De HBW strekt tot uitvoering van de EU verordening inzake het vergroten van de veiligheid van schepen en havenfaciliteiten. Normaal gesproken is de Trw niet van toepassing op wetten die strekken tot één op één implementatie van vastgestelde besluiten van de EU. Echter, de HBW strekt tevens ter implementatie van toekomstige besluiten van de EU of van andere volkenrechtelijke organisaties op het gebied van de beveiliging van havens. De HBW dient derhalve niet uitsluitend tot uitvoering van een reeds vastgesteld besluit van de EU. Daarom valt de HBW onder de Trw. (Zie verder voetnoot 23)

Inmiddels is eveneens een interdepartementale overleggroep gestart die ook door de plaatsvervangend DG van DGG wordt voorgezeten. Een belangrijk gespreksonderwerp hierbij is de doormandatering van de bevoegdheden van de minister van V&W aan lokale bestuursorganen die onder andere ministeries ressorteren.

De plaatsvervangend DG van DGG legt verantwoording af aan de minister van V&W en aan de Tweede Kamer. Bij afwezigheid neemt de DG van DGG waar. Hier komt een platte organisatiestructuur tot uiting.

3.9 Afsluiting

In dit hoofdstuk is uitvoerig ingegaan op de actoren die een rol spelen bij het securitybeleid in Nederland. Eén ding is duidelijk: het aantal actoren is groot, beperkt zich niet tot Nederland en is verspreid over de centrale en decentrale overheid en over particuliere organisaties en bedrijfsleven.
Een succesvol securitybeleid van DGG is dus op grond van een “optelsom” van deze actoren iets waarbij communicatie een essentiële rol speelt. Deze communicatie moet vanuit DGG zodanig worden georganiseerd dat er snelle en adequate toegang is tot de internationale en nationale organisaties die in beginsel niet of minder toegankelijk zijn voor particuliere organisaties. Verder is het van belang dat de verkregen informatie helder en éénduidig verspreid kan worden. Dit vergt niet alleen communicatie maar ook afstemming en coördinatie. De rol van de interne en externe actoren binnen het securitynetwerk is van groot belang en wordt in hoofdstuk 4 belicht.

4 Securitybeleid in de praktijk

4.1 Inleiding

Om te achterhalen wat de ervaringen zijn van zowel interne als externe actoren met de ontwikkeling en de implementatie van het securitybeleid binnen het maritieme cluster van DGG, zijn voor dit onderzoek 18 interviews afgenomen[17]. De vragen voor het interview zijn voor beide groepen actoren identiek[18]. In dit hoofdstuk wordt een analyse van de afgenomen interviews gemaakt. Deze analyse is verricht met behulp van het stappenplan van Price (2004: 331)[19] van paragraaf 2.2.

In paragraaf 2.3 van dit onderzoek is aan het stappenplan van Price een stap 0 toegevoegd. Daarin is beschreven dat terreuraanslagen in feite integraal onderdeel uitmaken van de maatschappij. Een dergelijke analyse is echter filosofisch van aard en laat zich nauwelijks vertalen tot een werkbare operationalisatie. Het is om deze reden dat stap 0 niet terugkomt in de vragenlijst die aan dit hoofdstuk ten grondslag heeft gelegen.

4.2 Preventie/risico's (Stap 1)

In deze stap wordt een onderscheid gemaakt tussen bedreigingen voor het maritieme cluster en maatregelen ter preventie van deze bedreigingen.

4.2.1 Bedreigingen

In deze subparagraaf komen de verschillende soorten bedreigingen aan de orde, zoals deze in paragraaf 2.2 zijn geïntroduceerd. Tevens zal hier de rol van de actoren in geval van een dreiging worden geschetst. Tenslotte volgt een conclusie.

Bedreigingen aan het schip, inclusief lading en passagiers
Terroristen kunnen een passagiersschip gijzelen om hiermee een bepaald doel te bereiken. Het schip is hierbij het doelwit voor terroristen. De IMO geeft juist hierom expliciete regelgeving die mondiaal van toepassing is.[20] De landen vertalen deze regelgeving vervolgens door naar maatregelen die rederijen van passagiersschepen moeten implementeren.

Ook kunnen verschillende terroristische groeperingen gebruik maken van zeeschepen, hetzij om er aanslagen op te plegen, hetzij om met behulp van kleine bootjes - die meestal zijn volgestouwd met explosieve lading - zelfmoordcommando's aanslagen te laten plegen.

Bedreigingen voor de infrastructuur
Het schade berokkenen aan de infrastructuur van de haven door een terrorist brengt enorm veel overlast met zich mee. Denk bijvoorbeeld aan overstromingen. Maar ook zijn er met name in de Rotterdamse haven veel objecten met een symbolische waarde: halverwege de Nieuwe Waterweg ligt

[17] Zie Bijlage 1: Respondentenlijst
[18] Zie Bijlage 2: Interviewvragen
[19] Zie paragraaf 2.2
[20] Deze richtlijnen zijn:
1. Assembly Resolutie A 584(14), getiteld: "Measures to prevent unlawful acts against passengers and crews on board ships. N.a.v. de kaping van de "Achille Lauro" is deze richtlijn gemaakt. Aangenomen op 20 november 1985.
2. Solas Chapter XI-2 en de ISPS-code. Opmerking: A584(14) heeft model gestaan voor deze richtlijn. Aangenomen in december 2002.

IMO heeft ook diverse circulaires (aanbevelingen) gemaakt over de nadere invulling van 1 en 2. Deze zijn *niet* bindend en analoog aan Part B van de ISPS-code.

bijvoorbeeld een enorme sluis die een terrorist naar twee kanten kan treffen. De handhaving van de openbare orde en veiligheid zal zeker bemoeilijkt worden. Als een terrorist een schip laat zinken in de Nieuwe Waterweg, dan levert dat niet alleen economische schade op, maar ook een maatschappelijk ontwrichting omdat aanvoer van onder meer levensmiddelen dan niet meer kan plaatsvinden.

Met name Europoort is van groot belang als doorvoergebied naar het Europese achterland. Het is evident dat zelfs de geringste verstoring – of het nou komt door een ongeluk of door opzet – grote gevolgen zal hebben. Als men daarnaast het feit in aanmerking neemt dat Europoort een belangrijke petrochemische concentratie van bedrijven laat zien, is dat een potentieel groot probleem.

De respondenten kwalificeren dit type bedreiging als “meest reëel”. Immers, terroristen kunnen met relatief weinig inspanningen en risico’s op het niet slagen van een aanslag toch een enorme impact teweeg brengen.

Bedreigingen voor de omgeving
Het schip kan worden gebruikt als wapen: een terrorist kan bijvoorbeeld een chemicaliëntanker laten ontploffen in een woongebied ergens in een haven of ergens bij de Botlek tunnel. Dit kan erg vervelende gevolgen hebben voor de verre omgeving.

Eigenlijk is een schip alleen dan maar bedreigend als wapen als het de kust nadert of als het in een haven ligt. Als het schip midden op de oceaan vaart en terroristen plegen een aanslag op dit schip, zal het schip weliswaar met man en muis vergaan, maar blijven de gevolgen voor de omgeving gering. Echter, als een aanslag wordt gepleegd op een olietanker, kan een grote milieuramp ontstaan. Hierbij kan gesteld worden dat de olietanker door terroristen als doelwit én als middel wordt gezien om een milieuramp te veroorzaken.

Bedreigingen door het vervoeren van materiaal voor aanslagen
Het risico bestaat dat terroristen met een gekaapt schip middelen transporteren die ingezet kunnen worden bij het plegen van een terroristische aanslag. Echter, het schip hoeft niet per se te worden gekaapt: het is ook mogelijk dat terroristen gebruik maken van zeecontainers op het schip om materiaal - bedoeld voor het plegen van een terroristische aanslag - te vervoeren. Ook het vervoeren van terroristen zélf kan via zeecontainers plaatsvinden.

Rol van actoren in geval van een dreiging
De bestuurlijke driehoek[21] besluit of er sprake is van een dreiging. Hieronder ressorteert een crisis/rampen/antiterrorisme-structuur die vervolgens in werking treedt. Deze beperkt zich in het kader van de preventie vooralsnog tot het nemen van preventieve maatregelen. In deze structuur, welke bestaat uit een bestuurlijke en uitvoerende laag, dirigeert de bestuurlijke laag de te nemen maatregelen. De uitvoerende laag komt pas in actie als er zich werkelijk een aanslag heeft voorgedaan. Hieraan voorafgaand worden natuurlijk wel extra beveiligingsmaatregelen uitgevoerd, welke nadrukkelijk als preventief aangemerkt moeten worden. De bestuurlijke driehoek stuurt de bestuurlijke keten aan. Deze keten bestaat uit het NCC, DCC’s en de burgemeesters. Deze keten stuurt ten tijde van een crisis de uitvoerende diensten aan, zowel op rijks-, provinciaal- als gemeentelijk niveau. Hierop wordt in de stap 3 nader ingegaan.

Grotere (lees: kwetsbare) bedrijven in Rotterdam worden middels een mobilofooninstallatie op de hoogte gebracht van de situatie. Deze bedrijven krijgen via de organisatie die de belangen van werknemers in de Rotterdamse haven behartigt 24 uur per dag informatie. Deltalinqs heeft hierbij een faciliterende rol.

Meer op het raakvlak tussen preventie en detectie kan het volgende worden genoemd:
Rederijen zullen in geval van een dreiging hun schepen gewoon laten blijven varen. Indien een rederij van mening is dat een dreiging specifiek tegen een schip van diezelfde rederij is bedoeld, worden al

[21] Deze wordt gevormd door de ministers van AZ, BZK en Justitie.

haar schepen ingeseind. Hierbij zal de rederij zich afvragen waarom een van haar schepen wordt bedreigd: heeft het schip de verkeerde haven aangedaan, heeft het iets met het schip te maken of heeft het iets met de vlag te maken, met de eigenaar of de lading aan boord? In alle gevallen wordt gecommuniceerd naar het hoofdkantoor van de rederij in Nederland. Als er sprake is van een dreiging, moet deze altijd bij de “company security officer” terechtkomen. Hij zal bepalen of de dreiging met andere partijen wordt gedeeld om zo ook anderen in staat van verhoogde paraatheid te brengen.

De rol van de juridische medewerkers van DGG is heel beperkt. Dit wordt echter anders als er een concrete dreiging is en de vraag speelt of er een wettelijke bevoegdheid bestaat om actie naar aanleiding van deze dreiging te ondernemen.

De inspectiedienst levert expertise op die gebieden waar zij een verantwoordelijkheid heeft, daar waar het gaat om het plannen van vergunningen, het continueren van die vergunningen en het leveren van advies ook vanuit de beleidsfunctie aan het veld. Deze inspectieactiviteiten zullen – voor zover daar securityaspecten aan zitten – ook in tijden van een dreiging gewoon doorgaan.

Conclusie ten aanzien van bedreigingen
In zijn algemeenheid is er sprake van een generieke bedreiging, aangegeven door de diverse bronnen zoals inlichtingendiensten. Deze bronnen zijn dusdanig gezaghebbend, dat aan de geloofwaardigheid van dergelijke meldingen niet getwijfeld hoeft te worden.

Hieruit kan doorgaans niet de conclusie getrokken worden dat een dergelijke dreiging uniform benaderd moet worden. Dit betekent dat voor de hier boven genoemde soorten bedreigingen geen uniforme conclusie te trekken is. Het bij de respondenten bestaande eenduidige beeld over de bedreigingen die zich in het maritieme cluster kunnen voordoen, kan derhalve alleen maar toegesneden worden op één van de specifieke terreinen.

Een generieke bedreiging mondt uit in een specifiek risico. In zijn algemeenheid kan gesteld worden dat er sprake is van maatwerk: aan de hand van “assessments” wordt het specifieke risico bepaald en worden de maatregelen die genomen moeten worden hierop afgestemd. In de praktijk heeft derhalve ieder schip en iedere “port facility” zijn eigen specifieke plan van aanpak, hoe te handelen tijdens bedreigingen.

Een specifiek risico is afhankelijk van de omstandigheden, zoals: de lading die vervoerd wordt, de voorafgaande havens die het schip bezocht heeft, de nationaliteit van zowel het schip als de opvarenden en de aard van de terminal en de bescherming daarvan (een gasterminal is kwetsbaarder dan een etsterminal). Dit komt tot uiting in de specifieke “risk-assessments” die zowel door het schip als door de terminal zijn uitgevoerd en die uitmonden in een “security-plan”. Ieder plan is uniek en dekt de omstandigheden waarin schip en terminal zich bevinden. Met andere woorden: een generieke dreiging mondt uit in specifieke maatregelen. Als kort voorbeeld hierbij: de constatering dat twee naast elkaar gesitueerde olieterminals - zoals in Rotterdam het geval is – niet precies hetzelfde zullen reageren op een generieke dreiging.

In het geval van een specifieke dreiging (er is informatie bekend over een specifiek doel) kan dit uitmonden in een generieke risico: een aanslag op de Botlek tunnel in Rotterdam legt de activiteiten van de gehele haven vrijwel stil. In dit geval zal er sneller naar het hoogste veiligheidsniveau opgeschaald worden.

4.2.2 Maatregelen ter preventie van dreigingen

In deze subparagraaf wordt de aanleiding tot het nemen van maatregelen geschetst. De maatregelen ter preventie van dreigingen - zoals deze in paragraaf 2.2 zijn geïntroduceerd - komen aan bod. Tevens worden hier de maatregelen behandeld die de respondenten wel of niet afdoende vinden en welke maatregelen de respondenten samen met DGG moeten doorvoeren. Tenslotte volgt een conclusie ten aanzien van de doorgevoerde maatregelen.

Aanleiding tot het nemen van maatregelen
Door de aanslagen in de VS op 11 september 2001 is Nederland zich bewust geworden van een dreiging voor Nederlandse doelen. Nederland is een redelijk aantrekkelijk doelwit: de economische activiteit met 1,2 miljoen mensen vlakbij de Rotterdamse havens, gekoppeld aan het feit dat in Rotterdam een enorme olieopslag aanwezig is, is voor terroristen een interessante locatie om aanslagen te plegen.
Ook legt de VS een grotere internationale druk op andere landen om maatregelen te nemen tegen deze bestaande dreiging. Deze druk wordt direct na 11 september 2001 vanuit de IMO mondiaal geïnitieerd.

De Taskforce Security is ingesteld om binnen een bepaald beleidskader de beveiliging van de keten te verbeteren. IMO versterkt ongetwijfeld het security-denken in de keten, want per 1 juli 2004 zal er een beveiligd schip ontstaan en wordt er een risico-"assessment" gedaan. Vanaf 1 juli 2004 zal de IMO-code namelijk moeten gaan werken. Het stimuleren van security-maatregelen bij andere modaliteiten komt zeker voort uit de IMO-code. Na deze implementatiedatum zal een vrachtauto, binnenvaartschip of trein ook security-maatregelen moeten hebben uitgevoerd. Immers, laatstgenoemde modaliteiten sluiten aan op de zeescheepvaart in de havens. Daarnaast zijn de Amerikanen na 11 september 2001 meer tot het besef gekomen dat ook een vrachtauto met gevaarlijke stoffen (zoals bijvoorbeeld chloor) gebruikt kan worden als een terroristisch middel. Los van de maatregelen die in IMO-verband worden opgelegd aan de lidstaten, is het "security denken" van evident belang voor alle betrokken partijen.

Het "Department of Homeland Security" werd direct na 11 september 2001 ingesteld. Dit was ondenkbaar vóór deze datum, ondanks dat een aantal jaren voor deze aanslagen analisten in de VS voorspelden dat de VS slachtoffer zouden worden van een terroristische aanval: alle aanwijzingen waren toen reeds aanwezig. Maar politiek gezien zou het gewoonweg niet mogelijk zijn geweest om vóór 11 september 2001 dergelijke enorme maatregelen te nemen zoals die na deze datum wel werden bewerkstelligd. Kennelijk was er simpelweg een dergelijke aanslag nodig! De boodschap die de VS nu richten aan haar bondgenoten is dan ook: wacht niet totdat een terroristische aanslag wordt gepleegd op Parijs of Rotterdam voordat je dezelfde noodzakelijke maatregelen gaat nemen zoals de VS die na 11 september 2001 heeft moeten nemen.

Over de "hoofd"aanleiding – 11 september 2001 - waarom de organisaties hun maatregelen namen bestaat geen enkel verschil in de antwoorden van de respondenten. Opvallend is wel dat veel respondenten de aanleiding vervolgens zagen vanuit druk die werd uitgeoefend om maatregelen te nemen. Daarbij wordt met name de bilaterale relatie met de VS, waarbij een stevig dreigement in de vorm van economische sancties aan de orde was, expliciet genoemd. Daarnaast wordt de positie in internationale gremia vaak als aanleiding om mee te doen genoemd.

Internationale maatregelen
De IMO en de ILO hebben na 11 september 2001 afgesproken dat de havens over de hele wereld moeten worden beveiligd. De identificatie van zeevarenden speelt hierbij een rol, maar ook de risicoanalyses van havens. De meeste aandacht gaat uit naar deze laatste categorie. Hoewel een kaderinstructie voor de IMO is opgesteld, staat hierin tevens een aantal elementen die eigenlijk van toepassing zijn voor de hele transportketen. Het "security denken" verbreden naar de havens is essentieel in deze. Het is zaak dat naast zeescheepvaart ook het wegvervoer, de binnenvaart en het spoorvervoer bewust is dat men hier aan moet denken. Het voordeel van internationale regelgeving – als gevolg van de IMO-richtlijnen - is dat dit de grootste kans geeft op een internationaal "Level Playing Field" voor zowel schepen als havens, waarmee oneerlijke concurrentie wordt tegengegaan. Het creëren van een "Level Playing Field" is één van de aspecten die nogal omstreden zijn. Schepen met een vervoerscapaciteit van meer dan 500 kiloton moeten aan de regels van de ISPS-code voldoen. Dit zijn vrijwel alle zeeschepen. Er zijn gebieden in de wereld (het Midden-Oosten, Noord-Amerika en Engeland voor een klein deel) met een verhoogd risico op het plaatsvinden van een terroristische aanval. Er zijn echter ook reders die alleen maar varen in gebieden met een laag risico: Finland, Zweden, Duitsland. De vraag is of deze laatste groep van reders ook moet worden verplicht de ISPS-maatregelen door te voeren.

Na 11 september 2001 is er in de VS een multidisciplinair continuïteitsplan gekomen. Dit is een plan dat is gemaakt voor de regio en specifiek is gericht op de betrokken autoriteiten waarin richtlijnen staan hoe met het bestaan van verschillende dreigingniveaus moet worden omgegaan. Een van de gevolgen hiervan is dat de Amerikaanse regering meer geld uitgeeft aan de "US Coast Guards"voor schepen en personeel. Een positief neveneffect hierbij is de betere coördinatie tussen locale autoriteiten in de VS.

Nationale maatregelen
Naast internationale maatregelen worden er ook de nodige nationale maatregelen genomen. Zo werkt een beleidsafdeling binnen DGG mee aan de IMO-regelgeving door deze te implementeren in de Nederlandse wetgeving. De juridische dienst voert in dit kader niet zozeer zelf maatregelen door, maar verleent wel haar volledige medewerking, inclusief prioritering en urgentieverlening aan het tijdig implementeren van het IMO-pakket.

Het DCC coördineert het proces en gaat uit van voorlichting, beheer en proces. Beheer kun je ook zien als beleid. DCC bewaakt het proces van crisismanagement dat is gestoeld op drie pijlers: de eigen crisismanagementorganisatie, beleid en voorlichting. Indien er een probleem is worden deze drie pijlers bij elkaar geroepen en gaat DCC aan de hand van wat zij hebben geïdentificeerd als een probleem, verder aan de slag.
In Nederland is een risicoanalyse gemaakt van de kwetsbare locaties[22]. Deze risicoanalyse staat weergegeven in een intern rapport van Rijkswaterstaat, Adviesdienst Verkeer en Vervoer (2001).

In analogie met wat er op 11 september 2001 in de VS is gebeurd, moet men volgens een van de respondenten weliswaar rekening houden met aanslagen op met name Amerikaanse objecten in Nederland, maar moet men zich er echter wel voor behoeden dat er een hype komt waarin men alles wil gaan beveiligen. Als men alles gaat beveiligen, beveiligt men eigenlijk niets.
De hele security-affaire is door de Amerikanen immers met veel geweld opgebracht. Het is een politiek besluit om deel te nemen aan de maatregelen zoals die nu indirect door de VS worden opgelegd. Het idee komt niet uit Europa. Nederland probeert – net als andere landen in de wereld - met zo weinig mogelijk kosten aan haar verplichtingen te voldoen.

In en nabij de Rotterdamse havens is de werkwijze na 11 september 2001 op zich niet veranderd. Echter, security heeft duidelijk meer aandacht gekregen: zaken waar voorheen minder aandacht aan werd geschonken – toegangscontrole, toegangsregistratie, identificatieplicht – zijn nu wel onderwerp van aandacht. Security stond eigenlijk altijd al op de agenda, maar na 11 september staat dit onderwerp hoger op de agenda. Na 11 september is de aandacht niet meer zozeer op de criminaliteitspreventie gericht, maar meer op hoe de risico's ten aanzien van een dreiging van een terroristische aanslag kunnen worden beperkt.

Maatregelen op het schip
Het invoeren van de ISPS-code houdt in dat er nog een aantal zaken moet worden geregeld voor de implementatiedatum. Echter, veel reders hebben al een heleboel zaken geregeld: van oudsher bestaat reeds het probleem van piraterij. Veel van de maatregelen die hiervoor zijn doorgevoerd kunnen één op één worden vertaald naar de maatregelen die voor de ISPS-code moeten worden geregeld.

Een andere respondent geeft aan dat de wereld wakker is geschud na 11 september 2001. Toen betrof het de luchtvaartsector, maar andere (vervoers)sectoren zijn even kwetsbaar. Vanaf deze datum is het balletje gaan rollen in Europees, IMO en nationaal verband. Er kwamen allerlei initiatieven, die moeten worden uitgevoerd. Als het goed is worden IMO-maatregelen en nationale maatregelen op elkaar afgestemd.

Het maritieme cluster is qua omvang en samenstelling niet veel veranderd na 11 september 2001. Er wordt na de aanslagen in New York echter wel een groot issue van de beveiliging van objecten en

[22] Geheime informatie.

personen gemaakt. Volgens een aantal respondenten doen met name de Amerikanen erg paranoia en wentelen de kosten van hun fobieën af op de rest van de wereld.

Maatregelen voor reders
De reders willen handel blijven drijven met de VS en met de andere "contracting governments". Deze reders zijn verplicht hun maatregelen door te voeren, anders worden ze buitengesloten door de VS. De Amerikanen hebben in de IMO voorstellen gedaan. Als deze voorstellen wereldwijd niet worden aangenomen – dus een reder probeert bepaalde zaken in zijn eigen voordeel om te buigen – komt de reder met zijn schip de VS niet meer in.

Maatregelen die respondenten wel of niet afdoende vinden
Een respondent geeft aan dat de betrokken actoren teveel gefocust zijn op het voldoen van de regelgeving sec, zonder aandacht te hebben voor hetgeen waartegen wij ons allemaal willen beveiligen. Essentiële vragen hierbij zijn: "Op welke manieren moet dat gebeuren?", "Kan het uitgevoerd worden?". Men moet zich "to the point" beveiligen en zich behoeden voor een "overkill" aan maatregelen. De "modus operandi" is zeer essentieel als je het hebt over security in het maritieme cluster. De kennis die er bij V&W en binnen de havens is op het gebied van beveiliging en op het gebied van wat men het beste kan doen bij het voorkomen dan wel het beperken van de negatieve gevolgen van een terroristische aanval, moet nauwer op elkaar aangesloten worden tussen de participerende actoren.
Alle actoren binnen het securitynetwerk zijn zich bewust van het moeten voldoen aan een beveiligingsplan en welke acties hierbij genomen moeten worden. Echter, de link naar de politie ontbreekt maar al te vaak. Tevens constateert de politie dat sommige organisaties een rampenplan "vertalen" naar een securityplan, wat duidelijk niet de bedoeling is.

Vanuit V&W centraal bezien wordt geconstateerd dat men op het gebied van safety al erg ver is, maar dat security eigenlijk nog in de kinderschoenen staat. Er moet nog heel veel zendingswerk worden verricht. Binnen de organisatie merk je ontzettend goed dat het ene onderdeel veel beter is voorbereid dan het andere onderdeel. Naast het te behandelen beleidsterrein, heeft dit echter ook te maken met de wet- en regelgeving.

De politieke en economische noodzaak heeft er voor gezorgd dat de sector goed meewerkt. Een aandachtspunt voor Nederland zijn de kleine havens en de kleine reders. Een kapiteineigenaar die niet naar de VS vaart, heeft een afwachtende houding. Echter, de IMO-code is mondiaal en vroeg of laat moet ook deze kapiteineigenaar zijn maatregelen hebben doorgevoerd.
Ook is in een aantal landen in West-Afrika de aandacht voor security onderwerpen veel minder. Verder heeft Latijns-Amerika te maken met hoge corruptie. In Rotterdam weet men dus lang niet altijd of een buitenlands schip wel veilig is.

Binnen DGG merkt een aantal respondenten op dat met name bij de wat kleinere havens in Nederland maar een zeer beperkt aantal mensen zich bezighoudt met safety en security. Dit kleine gezelschap moet alles wat hierbij komt kijken "maar allemaal behappen", kan dit echter veel minder snel dan de grotere organisaties. Immers, kleine organisaties zijn toch een beetje huiverig om te investeren, zowel in tijd als in geld.

Enkele respondenten zijn benieuwd naar de uitwerking en wachten op de implementatie. Zij missen eigenlijk geen maatregelen bij andere organisaties. De schepen, inclusief bemanning en mensen aan de wal moeten per 1 juli 2004 aan allerlei regels voldoen. Echter, hoe zaken op de schepen en in de havens zullen gaan lopen, is voor een aantal respondenten nog onvoldoende helder.

De Amerikanen zijn van mening dat de Nederlandse regering, locale overheden en de private sector het onderwerp van security erg serieus nemen. Niet alleen de security in het maritieme cluster, maar ook de bescherming van kritieke infrastructurele werken in nationaal opzicht. Ook het feit dat de ministeries in Nederland niet alleen met lokale overheden samenwerken maar ook met de private sector, wordt door de Amerikanen als een belangrijk voordeel gezien van de Nederlandse benadering.

Een aantal respondenten merkt op dat voor wat betreft de maritieme security er reeds vóór de implementatiedatum van de IMO al erg veel wordt gedaan door de sector zelf. Zowel de havenbedrijven als de reders zijn zeer actief. Op voorhand kunnen deze respondenten niet zeggen dat een direct betrokkene geen of onvoldoende aandacht besteedt aan het aspect van maritieme security. Voor de maatregelen die op 1 juli 2004 ingaan is het zo dat het niet voor iedereen binnen de sector concreet en helder is wat er nou precies moet gaan gebeuren om mensen klaar te maken voor het aspect van security in het maritieme cluster. Dit laatste is voor een groot deel te wijten aan het feit dat instanties zoals de IMO te laat met duidelijkheid komen over wat de te nemen maatregelen nou precies inhouden en wat de criteria exact zijn waaraan een reder per 1 juli 2004 moet voldoen.

Een respondent merkt in het verlengde van het voorgaande punt op dat er reeds een groot aantal maatregelen is doorgevoerd in het kader van piraterij. Dit is ook bestaand beleid, zeker bij DGG. Deze respondent vraagt zich af waarom de expertise die is opgedaan bij dit beleidsonderwerp niet verder is ingezet voor security vraagstukken.

De IMO bepaalt in grote lijnen welke maatregelen wereldwijd moeten worden ingevoerd om de havens van de VS te mogen blijven aandoen. Voor Nederland geldt dat de EU de vertaalslag voert tussen wat wereldwijd door de IMO wordt bepaald en hoe op Europees niveau aan deze IMO-richtlijnen invulling moet worden gegeven. De respondenten ervaren reeds in deze vertaalslag een belangrijke omissie. Immers, de EU heeft tot aan 1 juli 2004 onvoldoende duidelijkheid gegeven wat de rederijen moesten doen om aan de ISPS-code te voldoen: de rederijen wisten niet wat de exacte eisen waren ten aanzien van bijvoorbeeld het opleiden van de “company security officer” en de “ship security officer”. Ook was het voor dezelfde rederijen niet duidelijk welke eisen er aan het schip werden gesteld. Juist door deze onduidelijkheid ervaren de respondenten die direct of indirect te maken hebben met de implementatie van de IMO-richtlijnen het hele securitygebeuren, dat de Amerikanen na 11 september 2001 wereldwijd hebben gelanceerd, als “te ver doorgeslagen” en zijnde een “tijdelijke paniekreactie van de Amerikanen, die over een paar jaar wel weer is overgewaaid”.

Binnen TZ wordt met name bij het ministerie van Justitie een heleboel gemist. Volgens een respondent verricht het ministerie van Justitie onvoldoende acties en is alleen maar “eigenwijs” bezig. Zo probeert dit departement met de Amerikanen bilateraal overeenkomsten te sluiten, waar andere (Nederlandse) actoren geen weet van hebben. Dit wordt als bijzonder onaangenaam ervaren.
Een andere respondent bij TZ heeft het idee dat iedereen erg actief bezig is. De reders en de Rotterdamse havens spelen een voortrekkersrol. Werknemersorganisaties ook wel, maar die kijken meer “de kat uit de boom”. Zij zijn van mening dat deze problematiek een zaak van de overheid is en daar hebben ze volgens deze respondent ook wel gelijk in.

Het ministerie van Justitie wordt in deze door een andere respondent als puur reactief ervaren. Het OM in Rotterdam heeft veel geleerd volgens deze respondent en beseft inmiddels dat deze materie speciale aandacht en aanpak behoeft. Echter, bij de zittende magistratuur zie je – ook vanwege het feit dat mensen snel van baan wisselen – dat voor specifieke misdrijven die in de haven worden gepleegd, soms te weinig kennis voorhanden is. Je ziet heel vaak dat advocaten op een hele eenvoudige manier de rechtbank kunnen misleiden omdat de rechtbank onvoldoende zicht heeft op wat zo’n haven eigenlijk is.

HDJZ is van mening dat het ministerie van Justitie te weinig aandacht heeft voor maritieme onderwerpen. Dit departement kijkt, volgens deze respondent, naar wetgevingsproducten. Maar als het gaat om beleidsmatig-conceptueel, dan is Justitie in hoofdzaak gericht op het strafrechtelijke aspect. Binnen het ministerie van Justitie staat het security-onderwerp wel op de agenda, maar wordt daar louter door een strafrechtelijke bril bekeken.
Dezelfde respondent merkt op dat het Amsterdams bestuur niet voldoende is voorbereid om adequaat op een terroristisch aanslag te reageren. Dit komt, volgens deze respondent, omdat in Amsterdam de politieke aandacht voor de haven erg laag is. De Amsterdamse situatie staat haaks op de Rotterdamse. In Rotterdam is de havenwethouder na de burgemeester en de loco-burgemeester de meest prominente

wethouder, terwijl de havenwethouder in Amsterdam veel minder prioriteit toekent aan dit onderwerp. Deze Amsterdamse wethouder vindt de Noord-Zuid lijn namelijk veel belangrijker voor Amsterdam. Deze wethouder heeft de haven eigenlijk "erbij" gekregen in zijn takenpakket.

De vermeende geïsoleerde werkwijze van het ministerie van Justitie wordt aldus vaak genoemd door de respondenten.
Daarnaast refereren veel respondenten aan het feit dat security-regelgeving wordt gezien als het opnieuw uitvinden van het wiel, terwijl niet of nauwelijks wordt gekeken naar maatregelen en afspraken die in het kader van veiligheid en piraterijbestrijding reeds zijn gemaakt. Deze lacune in de aanpak wordt door veel respondenten als zeer ongewenst aangegeven.

Maatregelen die respondenten samen met DGG nog moeten doorvoeren
Alle respondenten vinden het zaak dat er een "Level Playing Field" moet worden gehouden. Dit betekent dat de havens in bijvoorbeeld Hamburg en Antwerpen dezelfde maatregelen moeten doorvoeren als de Nederlandse havens. Het mag niet zo zijn dat één land een veel hogere kostenpost heeft dan een ander land.

Een respondent geeft aan dat de "company security officer" breder opgeleid moet zijn dan de "ship security officer", die lokale kennis behoort te hebben. De "company security officer" behoort de regelgeving als zodanig te kennen en zal zich hierin moeten verdiepen. De teksten voor beide opleidingen zijn in vrij korte tijd tot stand gekomen en er zitten ongetwijfeld fouten dan wel onvolledigheden in die eruit gehaald moeten worden. Het is van belang dat er samen met DGG nog eens kritisch naar deze teksten wordt gekeken.
Het opleiden van mensen is in dit kader een actiepunt dat door een andere respondent wordt genoemd. Op de Haagse Hogeschool kunnen studenten zich bekwamen tot MBA in "Security Management". Dit betekent dat men allereerst aantoonbaar maakt dat men vakbekwaamheid in huis heeft. Ook laat het volgen van deze opleiding zien dat de verantwoordelijkheden serieus worden genomen.

Een respondent merkt op dat veel zaken die in dit kader effect moeten hebben veel beter zullen uitpakken als de overheid ze op vrijwillige basis uitzet (door bijvoorbeeld subsidies te verlenen), dan wanneer de overheid ze voorschrijft. De vraag hierbij is echter hoe flexibel het bedrijfsleven is en hoe flexibel de overheid met dat soort zaken om gaat.

Een respondent geeft aan dat er zeker nog een aantal zaken met DGG zijn te realiseren om te voldoen aan een veilig maritiem cluster. Echter hiervoor geldt: men moet het even de tijd geven, even aanzien wat er gebeuren gaat. Deze respondent wacht desondanks niet op de overheid om te zien wat er moet gaan gebeuren, maar geeft aan dat zijn organisatie zelf alvast doorgaat met het nemen van maatregelen. Immers, er moet een "security assessment" worden gemaakt van wat er nog gedaan moet worden: aan wal, aan boord van de schepen en met betrekking tot het opleiden van mensen. Als er gewacht moet worden op de overheid is de organisatie waar deze respondent werkzaam is veel te laat met het invoeren van haar maatregelen.

Enkele respondenten geven aan dat het van essentieel belang is dat de HBW vóór 1 juli 2004 in werking moet zijn getreden[23].

> *(Achteraf is gebleken dat deze datum niet is gehaald. V&W heeft een voorziening getroffen dat havenbeveiligingscertificaten hetzij door de minister van V&W (periode van 1 juli 2004 tot*

[23] De HBW is op 22 juni 2004 behandeld in de Tweede Kamer. Op 26 juni heeft de Tweede Kamer de HBW aangenomen. Op 5 juli 2004 heeft de Eerste Kamer het wetsvoorstel aanvaard. Publicatie van de HBW in het Staatsblad heeft op 15 juli 2004 plaatsgevonden. In concreto betekent dit dat de HBW op 21 augustus 2004 in werking treedt. Tot die datum blijft de voorlopige voorziening met betrekking tot de afgifte van verklaringen door de minister van V&W van kracht. Vanaf 21 augustus 2004 kunnen door de burgemeesters havenbeveiligingscertificaten afgegeven worden.
(Zie verder voetnoot 16)

aan de datum dat de HBW in werking treedt: 21 augustus 2004) hetzij door de burgemeesters (situatie na 21 augustus 2004) kunnen worden afgegeven.)

Een aantal respondenten deelt de mening dat security als communicatie en security als een onderdeel van training/opleiding van groot belang is. Men moet binnen het cluster veel meer "awareness" zien te bewerkstelligen. De marktpartijen en de overheidspartijen realiseren zich dat het heel kort dag is vóór de implementatiedatum. De communicatie richting ambtenaren en mensen die in de havens en op schepen werkzaam zijn is een lastige klus waar wellicht nog meer over nagedacht zou kunnen worden.

Gelet op bovenstaande antwoorden van respondenten, is het niet verwonderlijk dat integratie tussen het beleid op de terreinen van veiligheid, beveiliging, crisis en piraterij veel meer moet worden gestimuleerd. De bestaande kennis is voor een belangrijk deel reeds aanwezig, maar wordt onvoldoende benut.
De algemene lijn van de gegeven antwoorden is dat alle betrokken actoren er gezamenlijk naar moeten streven om de implementatie van de maatregelen van de IMO en de EU in nationaal opzicht te realiseren. In de IMO security code is vastgesteld wat per 1 juli 2004 internationaal in werking moet treden. Dit internationale regime moet vertaald worden in nationale wet- en regelgeving, wat een taak is van de juridische medewerkers van de overheid. Echter, de eisen zoals die in IMO-verband zijn beschreven laten ruimte over voor interpretatie: het zou fijn zijn als de eisen uniform en unilateraal geïmplementeerd zouden worden of in ieder geval geïnterpreteerd zouden worden. Hier dienen de betrokken organisaties nog de nodige acties op te nemen.

Conclusie ten aanzien van de doorgevoerde maatregelen
Globaal kan gesteld worden dat de respondenten met slechts één uitzondering allen de noodzaak tot het nemen van maatregelen niet ter discussie stellen. Opvallend daarbij is dat de maatregelen niet worden gerelateerd aan de mogelijkheid - of misschien beter de onmogelijkheid - of überhaupt maatregelen genomen kunnen worden tegen terrorisme. M.a.w. de maatregelen worden geïsoleerd bekeken en niet in een breder kader (bijv. politicologisch, sociologisch) geplaatst. Een zeer instrumentele benadering dus. Het beeld dat ontstaat is dat vrijwel alle respondenten de internationale context sterk benadrukken en dit doen vanuit het bewaken van het "Level Playing Field". Het is dan ook niet verwonderlijk dat de referentiekaders daarbij de internationale organisaties zijn. "Level Playing Field", coördinatie, goede afstemming en een goede implementatie van de maatregelen zijn de belangrijkste aandachtspunten.

4.3 Detectie (Stap 2)

Binnen de AIVD is maritieme security een apart aandachtspunt geworden. Echter, hier heeft dit niet zo'n hoge beleidsprioriteit gekregen zoals dat bij DGG het geval is. Dat houdt ook simpelweg verband met de beschikbare mankracht. De AIVD wisselt informatie uit met een heleboel organisaties, in feite met alle departementen. De respondent is van mening dat de AIVD zichzelf veel meer macht en invloed toeschrijft dan dat de AIVD feitelijk heeft. Hierover wordt binnen deze dienst verschillend gedacht. De AIVD is eigenlijk meer een soort van inspectiedienst die in de samenleving moet kijken en daardoor aan haar informatie komt. Het is aan de andere organisaties wat zij met deze informatie doen. Dáár ligt het zwaartepunt: de AIVD is eigenlijk een organisatie van toeleveranciers. Echter, in feite schrijft juist de politiek – in voorkomende gevallen – de mate van macht en invloed aan de AIVD toe. De AIVD zoekt contact met personen binnen DCC, waarbij DCC wordt geïnformeerd over bepaalde risico's. Het andere kanaal loopt via het Nationaal Coördinatie Centrum (NCC). Het is dan aan het NCC om te beoordelen wat er verder met de informatie wordt gedaan. Hier heeft de AIVD niet altijd controle op. In voorkomende gevallen informeert de AIVD ook wel eens de burgemeester van met name de grote steden in Nederland.

BUZA heeft eigenlijk geen actieve rol in deze en juist hierdoor staat deze organisatie op de verzendlijst van allerlei werkgroepen en overleggen. BUZA is verantwoordelijk voor het buitenlands beleid, maar op het moment dat de materie echt vakinhoudelijk wordt, is BUZA slechts coördinerend

en wordt het internationale transportbeleid of securitybeleid getrokken door het daarvoor ingestelde vakministerie. De initiatieven voor het nemen van allerlei securitymaatregelen komen volgens deze respondent bij V&W vandaan en die worden op hun beurt gevoed vanuit de sector, door BZK en deels door Justitie. Daarnaast zijn er allerlei internationale overleggen die ook nog spelen: internationaal gezien is de IMO hier actief mee bezig, maar ook in Europees verband worden veel besluiten genomen. In Brussel worden op Europees niveau maatregelen genomen die voor een groot gedeelte weer aansluiten bij wat er in IMO kader wordt besloten. Europa wordt steeds belangrijker en dat is iets waar de gemiddelde Europese burger, zich volgens dezelfde respondent, te weinig van bewust is. BUZA is een actor die meer op afstand staat van andere relevante actoren binnen het securitynetwerk. Deze positie heeft BUZA gekregen doordat zij de schaarse informatie die zij ontvangt van andere actoren ook niet doorstuurt naar anderen.

Het Departementaal Coördinatie Centrum (DCC) bestaat eigenlijk dankzij het feit dat deze dienst communiceert met andere organisaties. De organisatie van het DCC is dusdanig ingericht dat er overal crisiscoördinatoren zijn die het DCC direct kan bereiken. Daarnaast heeft het DCC contacten met andere departementen. De respondent stelt dat wanneer er morgen een aanslag wordt gepleegd door een terrorist, hij dat heel snel te weten komt. De respondent zal heel snel na de eerste analyse de ambtelijke en politieke top inlichten, alsmede de Directeuren-generaals en de regionale directies die binnen Rijkswaterstaat de betreffende risicogebieden bestrijken.

Een respondent die bij DGG, afdeling Zeescheepvaart (TZ) werkzaam is, vindt de rol van TZ bij deze stap onduidelijk. TZ heeft volgens deze respondent een meer signalerende functie: de procedures zijn inmiddels helder. Indien er sprake is van een reële dreiging dat loopt het kanaal via de AIVD, die vervolgens het NCC en het DCC en de bestuurlijke driehoek informeert. De driehoek bepaalt vervolgens wat er moet gebeuren.

De primaire rol van de Amerikaanse ambassade is het beschermen van haar ingezetenen in Nederland. Maar ook het bieden van hulp staat bij de Amerikaanse ambassade hoog in het vaandel. Vanwege het feit dat terrorisme een sterk internationaal karakter heeft, zijn er altijd relaties uit te kristalliseren met zaken die zich in andere landen afspelen. De Amerikanen werken samen met de Nederlandse autoriteiten om na te gaan hoe terroristen in andere landen betrokken zijn geraakt bij het voorbereiden van een terroristische aanval.

De politie zal haar waakzaamheid verhogen en informatiestromen kanaliseren. Zij zet haar mensen op scherp in het hele havengebied via de communicatiestructuren die daarvoor aanwezig zijn. Tevens voorziet de politie de AIVD van de nodige informatie.

Het Rotterdamse havenbedrijf heeft een erg faciliterende rol. Zij houdt haar ogen en oren open bij alles wat er in en om het water gebeurt, heel duidelijk uitvoeringsgericht. Zij werkt samen met de zeehavenpolitie en wisselt informatie uit met alle betrokken actoren. In het pand van voornoemde organisatie bevindt zich het havencoördinatiecentrum. Dat is de plek waar alle (elektronische) informatie bij elkaar komt en waarbij de mensen van de verkeersleiding zijn ondergebracht.

Deltalinqs heeft in Rotterdam de rol van doorgeefluik. Er zijn korte lijnen namens de bedrijven met politie en andere overheden.

4.4 Crisismanagement (Stap 3)

Bij deze stap wordt een onderverdeling gemaakt in:
- Type besluitvorming (paragraaf 4.4.1)
- Visie op de risico's (paragraaf 4.4.2)
- Soorten schades (paragraaf 4.4.3)

4.4.1 Type besluitvorming

Op het moment dat er een ontploffing heeft plaatsgevonden of er een schip tot zinken is gebracht, is het vooral een zaak van crisisbeperkende maatregelen. Dan geldt het noodscenario dat geldt voor een "security- of een safety-event", dat maakt op dat moment niets uit. Security is een manier van kijken naar de wereld – uitgaande van het ondenkbare – die in brede delen van bestuurlijk Nederland nog geen ingang gevonden heeft. Het zou voor heel veel beleidsmakers, mensen in de uitvoering en in de handhaving als bijna ondenkbaar gezien worden dat zich werkelijk zo'n gebeurtenis zou plaatsvinden. Het feit accepteren dat het mogelijk is, is de eerste stap op weg naar "security-awareness".
De AIVD wordt in zo'n geval geïnformeerd over wat er heeft plaatsgevonden. Vervolgens is het aan de AIVD om te verklaren vanuit welke hoek de aanval is gekomen.

Als er sprake is van een terroristische gebeurtenis waarbij een nucleair transport betrokken is, dan is de rol van bureau Nucleaire Beveiliging Scheepvaart (NBS)[24] groot. NBS heeft de leiding om het onderzoek uit te voeren. De minister van VROM is primair verantwoordelijk voor nucleaire transporten. Ook het NCC wordt ingeschakeld, want deze dienst participeert in het meldingstraject.
De rol van NBS binnen het security-netwerk is heel groot. NBS heeft de bevoegdheid om via het NCC het evaluatieoverleg in gang te zetten. Op grond van de uitkomsten die uit de evaluatiedriehoek komen, neemt NBS verdere acties. Volgens de respondent kan de macht en invloed van NBS heel groot zijn.

De burgemeester van een gemeente met een haven heeft de eindverantwoordelijkheid in het crisismanagement op lokaal niveau. Onder diens verantwoordelijkheid is een organisatie (waarvan de bestuurlijke structuur reeds belicht is) bestaande uit lokale instanties zoals politie, brandweer, GGD, havencoördinatiecentrum (HCC) en douane actief in een crisiscentrum. Hier worden de besluiten, welke nodig zijn om de crisis te bezweren, genomen. Deze besluiten en de ontwikkeling van de crisis als zodanig worden gecommuniceerd naar de provincie en het landelijke bestuursorgaan. De commissaris van de Koningin heeft in dit proces eigenlijk geen andere rol dan het vanaf de zijlijn toezien hoe de situatie zich ontwikkelt.
In de Rotterdamse situatie waar het havenbedrijf actief is op beleidsmatig, bestuurlijk en commercieel terrein, participeert deze slechts op bestuurlijk niveau in de afhandeling van een crisis. Het onder dit havenbedrijf ressorterende HCC – met de havenmeester en zijn bevoegdheden – is de werkelijke uitvoerder, zij aan zij met de andere hierboven genoemde uitvoerende instanties.
In andere havens is - afhankelijk van de grootte van de haven - in principe een soortgelijke structuur aanwezig, maar meestal kleinschaliger. Dit is gebaseerd op het gegeven dat de afhandeling van een crisis tot de verantwoordelijkheden van een burgemeester behoort.

De rol van de provinciale en landelijke crisisstructuur is op lokaal niveau beperkt: zij volgen de ontwikkelingen en extrapoleren indien de lokale situatie een bredere uitstraling dreigt te krijgen. Met andere woorden: zodra het lokale niveau overstegen wordt, komen de hogere echelons in actie. Bijvoorbeeld: indien een giftige gaswolk het bevoegdheidsgebied van de burgemeester van Rotterdam verlaat, komen de provincie Zuid-Holland en het NCC in actie omdat dan besluiten van grotere orde genomen moeten worden, zoals evacuatie, medische zorg, grootschalig transport, hulpgoederen enzovoorts.

Het DCC stuurt het proces van crisismanagement aan en zorgt ervoor dat alle betrokken aanwezigen tezamen een inventarisatie verrichten van de genomen maatregelen. Verder maakt het DCC een knelpuntenlijst van wat er allemaal mis kan gaan en wat er al misgegaan is. Ook maakt deze dienst het voor de andere betrokken actoren inzichtelijk waar het DCC wel en niet over gaat. Tenslotte legt het DCC de contacten met de andere departementen.

BUZA heeft hierbij eigenlijk geen rol, behoudens misschien een faciliterende en een coördinerende rol. Ook kan BUZA informatie verschaffen en internationaal contacten leggen via de ambassades. Maar eigenlijk zijn deze contacten voor een groot gedeelte al aanwezig in het bestaande netwerk.

[24] Bureau NBS is ondergebracht bij het ministerie van VROM.

De minister van V&W is verantwoordelijk voor het systeem van goederenvervoer. Indien er als gevolg van een terroristische actie een verstoring plaats vindt van dit systeem, wordt V&W betrokken bij het nemen van maatregelen om het systeem weer te goed te laten functioneren. De rol van de Taskforce Security is om dit proces in goede banen te leiden.

4.4.2 Visie op de risico's

Zoals eerder genoemd is een schip eigenlijk alleen dan maar bedreigend als wapen als het de kust nadert of als het in een haven ligt. Immers, bij een aanslag in of vlakbij een haven kunnen veel slachtoffers vallen en kunnen economische gevolgen erg groot zijn.
Als een aanslag wordt gepleegd op een olietanker kan midden op zee weliswaar een grote milieuramp ontstaan, maar dit wordt door een aantal respondenten echter als minder maatschappelijk ontwrichtend beschouwd.

Het feit dat er voor bulktransport geen alternatief is dan het transport hiervan via zeeschepen, gekoppeld aan het gegeven dat de luchtvaart meer met personenvervoer van doen heeft dan de zeevaart - op een enkel cruiseschip na – leidt er in de situatie zoals die nu is toe dat de uitvoerende partijen in het maritieme cluster hun reeds geïmplementeerde maatregelen te snel als "voldoende" afwikkelen. Immers, de uitvoerende partijen hebben niet van doen met een representatief vergelijkingskader.

4.4.3 Soorten schades

De respondenten onderscheiden hierbij een drietal soorten schades:

1 Imagoschade voor de Rotterdamse haven;
2 Economische schade: als een terroristische aanval goed wordt uitgevoerd zal de Rotterdamse haven zeker een paar weken onbruikbaar worden. Handelsstromen zullen verschuiven. Rotterdam zal de aanvoer niet meer aankunnen en men zal naar andere havens uitwijken. De internationale concurrentiepositie van Nederland zal verslechteren.
   Tevens kan economische schade ontstaan doordat er als gevolg van verscherpte maatregelen meer belemmerende wet- en regelgeving ontstaat;
3 Het gevoel van maatschappelijk onrust: het gevoel dat de Nederlandse samenleving kennelijk toch heel kwetsbaar is. Helaas is er een aanslag "nodig" om dit besef te creëren.

4.5 Herstel (Stap 4)

In Nederland is geen aanslag gepleegd. Dus van een herstel is geen sprake, in fysieke zin. Echter, de internationale regelgeving, voor een belangrijk deel geïnitieerd uit het herstel in de VS heeft ertoe geleid dat de ISPS-code ook voor Nederland geldt.

De rol van de politie in geval van een herstelperiode is divers: deze begint reeds bij de logistieke voorzieningen door gezamenlijk op te treden met andere overheidsdiensten zoals de brandweer. De primaire taak van de politie is het handhaven van de openbare orde en veiligheid. Tevens draagt de politie zorg voor het opstarten van het justitieel onderzoek: het inzetten van de recherchemedewerkers. Tot slot zal de hulpverlening op gang komen.

De Amerikanen zijn van mening dat de primaire verantwoordelijkheid bij de implementatie van de maatregelen die alle landen wereldwijd per 1 juli 2004 moeten hebben doorgevoerd, bij die landen zélf ligt. De VS stellen zich hierbij dienstbaar op door betrokken actoren van informatie te voorzien of door specifieke technologie in te zetten waarover de Amerikanen beschikken. De Amerikaanse ambassade bedeelt zichzelf een dergelijke coördinerende rol in. Immers, het zou niet de eerste keer zijn dat de Amerikanen hulp bieden in geval van een ramp c.q. oorlog in Nederland.

4.6 Integrale visie rondom informatie en communicatie in de keten

In deze paragraaf wordt dieper ingegaan op een aantal aspecten rondom informatie en communicatie over de keten (stap 1 t/m 4). Op een integrale manier wordt de algemeen gedragen lijn van antwoorden gegeven, waarbij de meest in het oog springende antwoorden geparafraseerd staan weergegeven:

De meeste respondenten verwijzen bij de beantwoording van de meest belangrijke organisaties om aan informatie over securitybeleid te komen naar de (bekende) internationale organisaties. De zusterorganisaties van particuliere organisaties, zoals de branchevereniging, worden echter niet genoemd. Er wordt uitsluitend gerefereerd aan de internationale organisaties, hetgeen zou kunnen betekenen dat “Level Playing Field” een centraal element vormt, dan wel dat het coördinatieaspect zo belangrijk wordt geacht dat via deze gremia het beleid kan worden bepaald.

Informatie-uitwisseling en bijbehorende rol binnen het maritieme cluster
Een respondent van TZ ziet de afdeling redelijk als een spin in het web: voor wat betreft de uitwerking van de IMO-afspraken participeert TZ in de meeste gremia. Ook de contacten met de KVNR zijn goed. Deze respondent bedeelt de afdeling binnen de sector dezelfde rol toe als zijn collega, namelijk die van beleidsmaker met een sturende rol. De taken die echt des overheids zijn, zijn in handen van TZ. Daarnaast heeft deze afdeling een combinatierol van sturend en faciliterend: de sector ondersteunen bij het optimaal benutten van kansen om een goede toegevoegde waarde te realiseren. Echter, volgens deze respondent was TZ hier in het verleden actiever in dan momenteel. Dit komt voornamelijk omdat de Taskforce Security een groot deel van deze taken heeft overgenomen.

De Taskforce Security heeft een actieve informatie-uitwisseling met een aantal omringende landen. Verder voert de Taskforce Security overleg met alle denkbare betrokken actoren in het veld: het bedrijfsleven, de havens, de havenraad, de reders, de redersvereniging, FNV Bondgenoten, Deltalinqs, de vereniging van havenmeesters, de Eigen Vervoers Organisatie (EVO), Nederland Distributie Land (NDL), enzovoorts.
Voor wat betreft macht en invloed is de Taskforce Security in eerste instantie verantwoordelijk voor de implementatie en de uitvoering van de nationale wet- en regelgeving op het gebied van security in het goederenvervoer. Zeker voor het IMO-gebeuren is de overheid “contracting-party” en in dit geval is dat V&W. De Taskforce Security heeft een aantal internationale verplichtingen op zich genomen en is met een aantal internationale organisaties bezig met het kweken van “awareness” voor de rest van de keten. De Taskforce Security schrijft achter de schermen mee aan voorstellen die in internationaal verband op tafel komen met betrekking tot security aangelegenheden in het maritieme cluster.

Met name de grote rederijen in Nederland wisselen onderling informatie uit. Ook met de overheid wordt informatie uitgewisseld. De rol van rederij Spliethoff kwalificeert de respondent als heel belangrijk, omdat deze rederij een koplopende functie heeft in deze materie. De respondent geeft aan dat veel rederijen Spliethoff volgen als het gaat om het nemen van maatregelen. Veelal zijn dit de kleinere rederijen. Het valt de respondent op dat er met het hele security-gebeuren heel veel openheid is onder elkaar: men hoort van elkaar wie wat doet of van plan is te gaan doen.

Een respondent van de Amerikaanse ambassade geeft aan dat er veel informatie-uitwisseling plaatsvindt tussen enerzijds de Amerikaanse regering en de Nederlandse regering en anderzijds de Amerikaanse ambassade in Den Haag en de Nederlandse ambassade in Washington. Dezelfde respondent bedeelt de Amerikaanse ambassade een faciliterende rol toe. Immers, er is op de Amerikaanse ambassade in Nederland geen grote groep van Amerikaanse analisten aanwezig en dat is ook niet de functie van de Amerikaanse ambassade. De Amerikaanse ambassade faciliteert in die zin dat zij probeert Amerikaanse en Nederlandse analisten zo nu en dan bij elkaar te brengen.

Een respondent van het Rotterdamse havenbedrijf is van mening dat de invloed van deze organisatie in de regio redelijk groot is. Het HBR is betrokken bij de afhandeling van het verkeer van nautische zaken en is eigenlijk met een heleboel andere denkbare processen actief in de haven. Veel bedrijven

kennen de organisatie. Het HBR is in een vroeg stadium begonnen met het security-gebeuren. Het geven van voorlichting en advies aan de bedrijven en publieke organen in de regio verricht het HBR middels door haar ingestelde adviesorganen. Organisaties kunnen vaak niet langs het HBR heen, maar het HBR kan ook niet zonder diezelfde organisaties. Als dat wel zo zou zijn, zou er niets gedragen worden door het veld en zou het HBR niets hoeven te coördineren.

De redersvereniging probeert daar waar het gaat om de implementatie van de regelgeving heel duidelijk sturend te zijn. De respondent geeft te kennen dat wanneer deze organisatie moet wachten op heldere en duidelijke antwoorden vanuit de overheid, deze waarschijnlijk toch veel te laat komen.

Vrijwel alle respondenten zien de organisaties waarin zij werkzaam zijn als onderdeel van het netwerk en geven dienovereenkomstig aan dat deze organisaties in termen van macht en invloed veelal een beperkte rol hebben. Opvallend is het feit dat vrijwel alle respondenten aangeven in het netwerk te zitten omdat zij door anderen worden aangesproken daarin deel te nemen.
Hoewel de netwerken door de respondenten als belangrijk worden gezien, wordt opgemerkt dat te vaak nog in afzonderlijke netwerken – bijvoorbeeld over piraterij, safety en security –wordt gesproken.

4.7 Afsluiting

In dit hoofdstuk zijn de 18 geïnterviewden uitvoerig belicht en is er een beeld van het securitybeleid in de praktijk ontstaan. Analoog aan de opzet van Price zijn de bevindingen gerangschikt. Met betrekking tot het dreiginggevaar ontstaat een eenduidig generiek beeld “er is een dreiging”, maar er kan worden geconcludeerd dat het specifieke risico in feite de kern vormt bij de respondenten. Daar worden uiteenlopende dreigingen geschetst, waarbij voor de havensector nadrukkelijk de economische schade - ook voor de langere termijn - in beeld komt.

Ten aanzien van de maatregelen is het duidelijk dat de in hoofdstuk 3 beschreven actoren hier veel werden genoemd. Het internationale kader werd veelvuldig genoemd, met als zeer opmerkelijk element dat de VS met economische sancties achter de hand een dominante factor vormen. De politieke en economische noodzaak zorgt er voor dat de sector goed heeft meegewerkt en nog meewerkt. De door de respondenten genoemde maatregelen varieerden van toegangscontrole, de invoering van de “ship security officer” en de “company security officer”, het scheppen van “awareness” tot aan een actie waar vrijwel alle respondenten het meest mee te maken krijgen: de invoering van de ISPS-code.
Zowel impliciet als expliciet is duidelijk dat er een goed ontwikkeld “awareness” niveau aanwezig is. Daarbij dient wel te worden opgemerkt dat vanwege de genoemde economische en politieke context het onduidelijk blijft of die “awareness” is ingegeven door reële dreiging dan wel door economische sancties (van de VS). Een aantal respondenten geeft aan dat met het wegvallen van eventuele sancties het in stand houden van de “awareness” problematisch wordt.

Opmerkelijk is dat er geen specifieke opmerkingen worden gemaakt over de coördinatie en communicatie, anders dan wat betreft het specifieke MKB-kenmerk van een deel van de sector. Deze bedrijven zijn in absolute zin te gering van omvang om de securityproblematiek integraal te betrekken bij de bedrijfsvoering. Bovendien is er bij het MKB weinig aandacht voor het securitybeleid als zodanig, behalve daar waar het gaat om verplichte maatregelen zoals de invoering van ISPS-code.

Voor alle respondenten geldt dat zij van de overheid en van internationale organisaties de meeste informatie ontvangen. Veel respondenten geven aan dat informatiestromen zo snel gaan dat vaak uit meerdere bronnen dezelfde informatie snel bij hen terechtkomt. Het gaat hierbij vooral om de internationale organisaties: IMO en EU en de nationale organisaties: AIVD, BZK en V&W.
In hoofdstuk 5 worden de bevindingen uit dit hoofdstuk afgezet tegen de uitgangspunten en veronderstellingen in hoofdstuk 2 en in mindere mate hoofdstuk 3.

5 Conclusies en aanbevelingen

5.1 Inleiding

Dit slothoofdstuk gaat in op de conclusies en aanbevelingen die gedurende het onderzoek naar aanleiding van de probleemstelling naar voren kwamen. In paragraaf 5.2 wordt een antwoord gegeven op de deelvragen zoals die in het eerste hoofdstuk van dit onderzoek staan vermeld. In paragraaf 5.3 wordt een antwoord worden gegeven op de centrale vraagstelling van dit onderzoek door de kernantwoorden van de deelvragen te koppelen aan de gebruikte theorieën en het veldwerk van dit onderzoek. In de laatste paragraaf van dit hoofdstuk staan de aanbevelingen beschreven.

5.2 Antwoord op de deelvragen

In paragraaf 1.2 zijn de volgende zes deelvragen geformuleerd:

1. Hoe ziet het securitybeleid van het maritieme cluster van DGG eruit en hoe is dit beleid georganiseerd?
2. Welke externe actoren zijn betrokken bij het securitybeleid van DGG?
3. Wat zijn conform het securitybeleid de taken en rollen van de interne en externe actoren?
4. Welke taken en rollen vervullen de interne en externe actoren nu werkelijk?
5. Hoe ervaren de externe actoren het securitybeleid van DGG?
6. Is er sprake van een informatie-uitwisselingsysteem tussen de partijen? Hoe is dit vormgegeven en zijn er mogelijkheden om partijen met elkaar in contact te laten komen en op welke manier kan dit worden vormgegeven?

De kernantwoorden van deze deelvragen zijn als volgt:

Na de gebeurtenissen van 11 september 2001 werden de bestaande structuren in het kader van het crisisbeleid als het ware gerevitaliseerd. Dit betekende dat de bestaande structuur gereactiveerd werd. Tegelijkertijd werd met deze structuur als het ware het fundament gelegd voor een versterkte structuur die het securitybeleid moest gaan dragen. Met name de internationale dimensie werd sterk versterkt, terwijl binnen het departement een coördinerende rol werd toebedeeld op het niveau van plaatsvervangend Directeur-generaal. Daarnaast werd gebruik gemaakt van expertise op de “werkvloer” om ervaringen die waren opgedaan in andere internationale gremia (i.c. de IMO) ook hier goed te kunnen borgen.
Evenwel bleek met name vanuit maatschappelijke onrust en (buitenlandse) politiek, maar vooral door economische druk dat de organisatiestructuur op zich te beperkt was om adequaat antwoord te geven op de gestelde eisen.
Het securitybeleid van DGG ontwikkelde zich snel door het instellen van een zwaar bemande werkgroep die op haar beurt zowel binnen het maritieme cluster als binnen nationaal en internationaal geactiveerde netwerken paste.

De externe factoren die betrokken zijn bij het beleid van DGG zijn nationaal te onderscheiden in mededepartementen, brancheorganisaties en andere particuliere organisaties. De mededepartementen die sterk betrokken zijn bij het beleid van DGG zijn het ministerie van Justitie en - wellicht nog belangrijker - het ministerie van BZK. Met betrekking tot brancheorganisaties is het met name de KVNR die een trekkende rol heeft gespeeld daar waar het gaat om het aanleveren van kennis van individuele ondernemingen en het verspreiden van de informatie naar die individuele ondernemingen toe. Ook hier is sprake van een verhoogd activiteitenniveau ten gevolge van de gebeurtenissen van 11 september 2001. Tot slot zijn het met name de havenbedrijven, zowel gemeentelijke- als particuliere organisaties, die betrokken zijn geweest bij de totstandkoming van het DGG-beleid. Internationaal was het reeds het gremium van de IMO dat na 11 september 2001 zwaarder werd opgetuigd, terwijl de EU in hoog tempo een coördinerende rol op zich nam.

De taken en rollen van de interne en externe actoren liggen vooral op het terrein van coördinatie, informatieverstrekking en communicatie. De mededepartementen – met name het ministerie van BZK - hebben naast de informatieverstrekking vooral een coördinerende taak. Zo filteren zij de informatie en informeren op basis van de gefilterde informatie het politieke crisisteam dat onder leiding staat van de minister van BZK. Bij de KVNR en de gemeentelijke- en particuliere havenorganisaties ligt het accent op het uitwisselen van informatie en het toetsen op realiseerbaarheid van DGG-voorstellen met het oog op een adequate realisatie van wetgeving die hen zou kunnen raken. De internationale organisaties hadden naast de introductie van nieuwe regelgeving vooral een coördinerende rol, die vanuit een “Level Playing Field” werd ingegeven.
Alle hierboven beschreven taken en rollen worden als zodanig ook daadwerkelijk ter hand genomen door de genoemde organisaties. Met betrekking tot de mededepartementen heerst er welhaast traditionele rivaliteit tussen het ministerie van Justitie en het ministerie van BZK. Voor de brancheorganisaties, gemeentelijke havenbedrijven en de particuliere organisaties in de havens (Deltalinqs) blijken de rollen zoals ze hierboven zijn beschreven ook redelijk te worden ingevuld. Hooguit kan hier de opmerking worden gemaakt dat een te passieve opstelling van deze organisaties in de ogen van de VS zou kunnen worden uitgelegd als het ontbreken van medewerking aan de ten uitvoer legging van regelgeving met alle mogelijke negatieve economische sancties van dien. De IMO heeft traditioneel een rol als bevoegd gezag op het terrein van internationale maritieme aangelegenheden en vervult bij deze aangelegenheid die rol dan ook. De EU, met in feite een regionaal belang (Europees), speelt een opmerkelijk uitgesproken rol bij de totstandkoming van de nieuwe havenrichtlijn.

Het securitybeleid van DGG wordt in algemene zin positief ervaren door de externe actoren. Zowel van de zijde van het ministerie van Justitie als dat van het ministerie van BZK wordt redelijk tot positief gesproken over het securitybeleid van DGG. Uitgesproken positief zijn de KVNR en de andere havenorganisaties over het securitybeleid van DGG. Met name op het terrein van de informatieverstrekking wordt DGG als goed beoordeeld. Als kritiekpunt geven de externe actoren aan dat er veel richtlijnen door de IMO en de EU werden ontwikkeld, maar dat het vaak bleef bij te vage richtlijnen. Ook voor DGG was het vaak niet duidelijk wat precies de gevaren zijn en waren en wat er precies geïmplementeerd moest worden. Om deze redenen kregen de externe actoren maar al te vaak geen helderheid omtrent de criteria van de te implementeren maatregelen en werd het implementatieproces onnodig vertraagd.
Noch van de EU, noch van de IMO is bekend wat hun oordeel is. Maar gelet op het feit dat Nederland voorop loopt bij de implementatie van de richtlijnen van deze organisaties, mag worden geconcludeerd dat het oordeel van beide organisaties positief zal zijn.

Securitybeleid in de huidige hoedanigheid is een nieuw fenomeen in Nederland. Security is een manier van kijken naar de wereld die in brede delen van bestuurlijk Nederland nog geen ingang heeft gevonden en waarbij uitgegaan wordt van het ondenkbare. Het wordt door heel veel beleidsmakers, mensen in de uitvoering en in de handhaving als bijna ondenkbaar gezien dat in Nederland soortgelijke aanslagen kunnen worden gepleegd zoals die op 11 september 2001 in de VS. Het feit accepteren dat dergelijke aanslagen in Nederland wel mogelijk zijn, is een eerste stap op weg naar “security-awareness”.
Juist een breed gedragen bewustzijn in Nederland zorgt ervoor dat onder een groot aantal betrokken medewerkers, zowel bij publieke- als private organisaties, voor een groot deel het gevoel wordt weggenomen dat de securitymaatregelen slechts als “noodzakelijk kwaad” worden gezien. Ten tijde van internationale “awareness” loopt het securitybeleid binnen DGG goed omdat er vanwege politieke en economische druk bij alle partijen bereidheid bestaat elkaar te informeren.

De informatie-uitwisseling tussen de partijen wordt als “goed” gekwalificeerd. Wel wordt opgemerkt dat met de huidige communicatiemiddelen dezelfde informatie vaak meerdere malen wordt aangeboden. Vrijwel elke organisatie heeft zijn eigen netwerk en die netwerken “dubbelen” elkaar, waardoor dit “probleem” ontstaat. Met betrekking tot afstemming en voorlichting werden reeds bestaande formele kanalen gebruikt die zijn gereactiveerd of werden nieuwe structuren opgezet. Het is

in dit kader van belang op te merken dat de aandacht die securitybeleid krijgt, of heeft gekregen zich niet één op één behoeft te vertalen binnen volledig nieuwe kennisuitwisselinginfrastructuren.

Met betrekking tot specifieke wet- en regelgeving kan worden gemeld dat ondanks het hoge tempo waarin regelgeving tot stand is gebracht - meer nog dan in het verleden het geval was - er een nauwlettender afstemming tussen zowel privaatrechtelijke als verantwoordelijke publiekrechtelijke organen plaats vindt.

5.3 Antwoord op de centrale vraagstelling

De kernantwoorden op de zes deelvragen zoals die in de vorige paragraaf staan omschreven, gekoppeld aan de gebruikte theorieën en het veldwerk van dit onderzoek, leveren het volgende beeld op voor de beantwoording van de centrale vraagstelling:
De centrale vraagstelling van dit onderzoek is:

> "Hoe vindt de ontwikkeling en de implementatie van het securitybeleid binnen het maritieme cluster van DGG plaats na de gebeurtenissen van 11 september 2001."

Om deze vraag te beantwoorden, is er binnen dit onderzoek een theoretisch kader ontwikkeld. Enerzijds bestond dat uit de basistheorieën uit de bestuurskunde zoals die door Rosenthal zijn weergegeven. Daarnaast is Perrow vanwege de risicoanalyse uitvoerig behandeld. Doorvertaald naar het veldwerk betekent deze invalshoek dat naast voor de hand liggende "bestuurskundige theorieën" impliciet Perrow aan de orde is geweest daar waar het gaat om het plaatsen van het begrip dreiging door terrorisme. Met één uitzondering geven alle respondenten aan dat veiligheidsrisico's en security-risico's binnen het maritieme cluster konden ontstaan en dat beleid ter vermindering van deze risico's moest worden ontwikkeld. Blijkbaar - in analogie met de analyse zoals die door Perrow is aangegeven - wordt het maritieme transport als een risicofactor gezien, die zich door de respondenten moeiteloos in het derde kwadrant laat plaatsen. Met hun antwoorden geven vele respondenten aan dat informatie-uitwisseling, afstemming en coördinatie zich afspelen binnen netwerken, dat deze netwerken onderling verbonden zijn met andere netwerken, dat coördinatie en afstemming bij voortduring aandacht vraagt en dat de economische context ("Level Playing Field") daarbij een belangrijke randvoorwaarde is. Met andere woorden: er is sprake van complexe interacties en "loose-coupling".

Met betrekking tot Douglas & Wildawsky en de respondenten ontstaat het beeld dat de problemen technisch van aard zijn en met betrekking tot de mate van overeenstemming de oplossing van deze problemen richting "complete" gaat. Een vertaling van de antwoorden van de respondenten op dit terrein betekent dus dat zij in het eerste kwadrant van het schema van Douglas & Wildawsky geplaatst kunnen worden. Opmerkelijk is het dus dat er een forse discrepantie ontstaat tussen de uitkomsten van de interviews en het theoretisch kader toegespitst op Douglas & Wildawsky. De respondenten ervaren de problemen als technisch van aard en zijn van mening dat ze de oplossingen in feite kunnen berekenen. De conclusie luidt derhalve dat de premisse bij Douglas & Wilawsky uit het tweede hoofdstuk niet houdbaar is: sluit men willens en wetens de ogen voor de complexe materie of is de materie eigenlijk niet zo complex?

Theoretisch voldoet het begrip "marine-transport" van Perrow niet aan het eerste kwadrant van Douglas & Wildawsky, terwijl de respondenten vrijwel unaniem "aangeven" juist in het eerste kwadrant van Douglas & Wildawsky te passen. In hun analyse gaan zij er van uit dat de middelen en de doelen met betrekking tot de benadering van het securitybeleid helder en adequaat kunnen worden beschreven. In die zin zou – vanuit de respondenten geredeneerd – zonder de waarheid daarbij enig geweld aan te doen, een dergelijk "wereldbeeld" zich goed laten lenen voor een eenvoudige bestuurskundige analyse waarbij doelstellingen en middelen overzichtelijk en zelfs uitputtend kunnen worden opgenoemd.

In het theoretisch kader is het derde kwadrant van Perrow in feite het kwadrant dat het meeste recht doet aan de complexe situatie van het maritieme cluster.
Vanuit die optiek zou verwacht mogen worden dat de respondenten met betrekking tot hun analyses op zijn minst met grote reserves over de problematiek de vragen zouden beantwoorden. In hoofdstuk 4 is aangegeven dat dit niet het geval is. Dit zou kunnen betekenen dat met de nodige veranderingen ook voor Perrow op grond van de bevindingen een ander kwadrant van toepassing is. Uit de antwoorden van de respondenten over de bedreigingen en de maatregelen komt een grote variëteit naar boven. Iedere respondent heeft een goed en allesomvattend beeld dat bij zijn of haar organisatie past. “Daar voor staan ze aan de lat” zou de populaire vertaling zijn. Ook hier wordt de problematiek gereduceerd tot hanteerbare proporties en is het eerste kwadrant van Perrow het meest bruikbaar.

Interessant is nu de vraag of het overheidsbeleid als zodanig zich ook op basis van de bevindingen in hoofdstuk 2 en de antwoorden van de respondenten zich zo eenvoudig laat rubriceren. Wederom wordt hier beklemtoond dat het in dit onderzoek besproken beleid niet het acute crisisbeleid is, waarbij onder zeer hoge druk ingrijpende besluiten moeten worden genomen. Het merendeel van de respondenten geeft aan dat economische druk vanuit de VS een belangrijke dwingende randvoorwaarde is geweest om te komen tot een securitybeleid. Vervolgens geeft men aan dat er aan een aantal randvoorwaarden moet worden voldaan. Goede informatie-uitwisseling, heldere overlegstructuren, communicatie tussen bestaande gremia (IMO en EU) worden daarbij als belangrijkste randvoorwaarden gezien die een goed securitybeleid kenmerken. Met betrekking tot de rolverdeling tussen overheid en private partijen bestaat nauwelijks verschil van mening over de invulling. De kaderstellende overheid en de implementerende private partijen vullen elkaar welhaast naadloos aan.
Vanuit de organisatieopzet in hoofdstuk 2 is aangegeven dat communicatie en coördinatie van groot belang zijn. Aangegeven is dat er zeer veel interne en externe actoren betrokken zijn bij de besluitvorming of maatregelen die daaruit voortvloeien. Aangegeven werd dat bestaande instituties op het terrein van crisisbeheer en beleid letterlijk werden opgeschaald veelal tot het niveau van een topambtenaar. Voorts is inzichtelijk gemaakt hoe de communicatie en coördinatiestructuren lopen. Er wordt gebruik gemaakt van reeds bestaande structuren die zwaarder worden opgetuigd of meer bevoegdheden krijgen.
Uit de antwoorden van de respondenten zijn geen kritische geluiden opgetekend daar waar het gaat om een gebrek aan communicatie en coördinatie. Gesteld mag worden dat er een positief beeld hierover bestaat en dat ook hier er niet wordt gesproken over complexe materie. Vanuit dat oogpunt ontstaat er een beeld van een overzichtelijk opererende overheid.
In het theoretisch kader werd de rationeel-synoptische benadering - in feite via een proces van eliminatie - als de meest voor de hand liggende theorie bij crisisbeleid aangegeven. Met de bevindingen uit hoofdstukken 3 en 4 kan hier op worden afgedongen.
Veel is te zeggen voor de incrementele benadering van Lindblom. Met name daar waar hij spreekt over “de concentratie op bekende en vertrouwde alternatieve mogelijkheden” en de oriëntatie op een marginale verbetering van de bestaande situatie”.
Als gekeken wordt naar de centrale vraagstelling leiden deze bevindingen ertoe dat de wereld-problemen eenvoudiger worden waargenomen dan de meeste mensen denken. Complexe - in feite ongrijpbare - problemen worden gereduceerd tot behapbare situaties waar maatregelen tegen genomen kunnen worden. Het zijn deze enigszins cynische bewoordingen die zich op basis van de empirie opdringen.

Er kan niet anders geconcludeerd worden dat DGG haar zaken goed op orde heeft. Juist de coördinatie en informatievoorziening - in feite de kerntaak - wordt positief beoordeeld. De interne maatregelen die zijn genomen met het opschalen van het “traditionele crisisbeleid” naar een steviger en meer politiek orgaan leidt er toe dat adequaat maatregelen worden voorbereid en uitgevoerd. Vastgesteld lijkt te kunnen worden dat deze positieve conclusie mede kan worden getrokken omdat de “awareness” ten tijde van dit onderzoek hoog was. De vraag is echter of deze vaststelling in de toekomst hetzelfde zal zijn.

Tot slot
Hoezeer het ook gewenst is om (ook) dit onderzoek af te sluiten met een synergie tussen bestuurskundige theorie, sociologische analyse en een uitgebreid veldwerkonderzoek, een eenduidig antwoord op de centrale vraagstelling is niet te geven zolang geen specifiek nauwkeurig omschreven beeld wordt gevormd omtrent het aggregatieniveau van de analyse: bij het betrekkelijk één op één aangeven van doelen en middelen is het beeld dat ontstaat redelijk helder, maar bij een meer abstracte analyse wordt het beeld diffuser omdat daarbij de doeleinden minder scherp zijn omschreven en in ieder geval de middelen als ontoereikend zullen worden gekenschetst. Dit kan als volgt worden toegelicht:
In dit onderzoek is aangegeven dat het maritieme cluster - zoals dat in dit onderzoek wordt gezien - in het derde kwadrant van het kwadrantenschema van Perrow valt. Een dergelijke indeling zou veronderstellen dat de bestuurskundige analyse er toe moet leiden dat slechts een theorie kan worden toegepast die een reflectie vormt van de plaatsing in dit kwadrant. Deze theorie zou dan als kenmerk dienen te hebben dat alternatieven en keuzes beperkt zijn, moeilijk kunnen worden voorzien en zich moeilijk laten vatten in uitgesproken theorieën. De theorie van de bevredigende oplossing zou dan kunnen worden "toegepast" omdat de bestuurders handelen op basis van ervaringskennis. De complexiteit is dermate hoog dat er vrijwel geen andere theorieën van toepassing zijn. Op basis van de analyse van de respondenten ontstaat evenwel een ander beeld. In algemene zin kunnen de antwoorden worden samengevat tot redelijk heldere doelen en welomschreven in te zetten middelen. Vanuit die optiek is de rationeel-synoptische methode een voor de hand liggende "match". Het is dus van cruciaal belang aan te geven vanuit welk aggregatieniveau geconcludeerd gaat worden, zodanig dat vanuit een bestuurskundige optiek aan dit onderzoek iets kan worden toegevoegd. Met betrekking tot de te nemen maatregelen wordt het probleem in een zeer complexe interactieve omgeving gereduceerd tot een entiteit die uitvoerbaar is en waarop bestuurskundige theorieën van toepassing zijn. Het is opvallend dat geen der respondenten zich uitgesproken heeft uitgelaten over nut en noodzaak van de te nemen maatregelen. Geen der respondenten heeft in analogie met bijvoorbeeld Perrow gemeend de onderhavige problematiek te moeten plaatsen in een bredere context, waarbij de doelen en middelen aanzienlijk moeilijker zijn te omschrijven. Het is deze essentiële notie die dit onderzoek heeft opgeleverd.

5.4 Aanbevelingen

Op grond van dit onderzoek kan een aantal aanbevelingen gedaan worden voor organisaties die in het securitybeleid binnen het maritieme cluster van DGG een toonaangevende rol hebben:

- De respondenten die het hele securitygebeuren ervaren als "te ver doorgeslagen" en als "een tijdelijke paniekreactie van de Amerikanen, die over een paar jaar wel weer is overgewaaid" zouden wellicht positiever hebben gereageerd als de betrokken partijen meer duidelijkheid hadden gekregen over wat er van hen werd verwacht. Betrokken partijen zouden dan zeer waarschijnlijk de te nemen maatregelen met een meer gedragen gevoel implementeren. Zowel de IMO, de EU en de nationale overheid (hier: DGG) hadden er wellicht beter aan gedaan de betrokken partijen – al ruim voor 1 juli 2004 - goed te informeren over het nut en de noodzaak van het implementeren van de securitymaatregelen;
- Voor de toekomst zal een redelijk goed functionerend informatienetwerk voor het securitybeleid van DGG moeten worden behouden omdat daarmee ook in een situatie die minder dreigend is, effectief beleid kan worden gevoerd. Tevens zal - analoog aan het onderhouden van "awareness" - op het terrein van crisis en rampenbestrijding in het stappenplan van Price, stappen 1 en 2 onderhouden moeten worden in geval van een dreiging van een terroristische gebeurtenis. Ook indien er geen sprake is van een terroristische gebeurtenis dient op dezelfde manier met de "awareness" ten aanzien van terrorisme gehandeld te worden. Tijdens stap 3 is het onderscheid tussen terrorisme en een andere maatschappelijke dreiging op het terrein van veiligheid niet meer van belang en het verdient aanbeveling dat de betrokken actoren zich hiervan bewust zijn en blijven. Een centraal aansturend orgaan – het meest voor de hand liggend is het NCC – zou met de betrokken actoren in het securitynetwerk kunnen overleggen op welke wijze zij "awareness"

geagendeerd houden. Voorts dient te worden onderzocht of er methoden zijn die als “best practise” kunnen worden gehanteerd. De keuze van “best practise” kan vervolgens worden verbreed naar andere organisaties;

- Het politieke gewicht van de nieuwe securitymaatregelen dreigt een aanslag te vormen op de noodzakelijk geachte reductie van de administratieve lasten. Vanuit V&W zal niet alleen handhaving en naleving van de ISPS-code een politiek belangrijk element moeten zijn, maar zal tevens moeten worden gelet op de bruikbaarheid voor de individuele ondernemers van de nieuw te implementeren maatregelen. Voorkomen moet worden dat nieuwe regels leiden tot een grotere administratieve lastendruk.

Bibliografie

Literatuur

Allison, G. & Zelikow, P. (1999). *Essence of Decision. Explaining the Cuban Missile Crisis.* New York, Longman.

Bachrach, P. en Baratz, M.S. (1963). Decisions and Nondecisions: An Analytical Framework, in: *American Political Science Review, 57. Power and Poverty.* New York, Oxford U.P.

Besier, G. (2002). *Niet … maar poetsen. Plan van aanpak "Maritieme Security".*

Beck, U. (1992). *Risk Society. Towards a new modernity.* London, Newbury Park (California), New Delhi, Sage publications ltd.

BVD (2001). *Terrorisme aan het begin van de 21e eeuw; dreigingsbeeld en positionering BVD.* Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, april 2001.

Commissie van de Europese Gemeenschappen (2003). *Voorstel voor een Verordening van het Europees Parlement en de Raad betreffende de verbetering van de beveiliging van schepen en havenfaciliteiten (door de Commissie ingediend). COM(2003) 229 definitief. 2003/0089 (COD).* Brussel, 2 mei 2003.

Docters van Leeuwen, A. et al. (2003). *Een kwestie van uitvoering. Vernieuwingsagenda voor de presterende overheid,* februari 2003.

Douglas, M. en Wildawsky, A. (1982). *Risk and Culture. An essay on the selection of technical and environmental dangers.* Berkely and Los Angeles, University of California Press.

Dror, Y. (1968). The Pure rationality model, in: *Policymaking Re-examined.* Scranton, Chandler.

Etzioni, A. (1968). *The Active Society: A Theory of Societal and Political Processes.* New York, Free Press.

Garland, D. (2003). The Rise of Risk, in: Ericson, R. & Doyle, A. *Risk and Morality*. Toronto, University of Toronto Press. pp. 48 – 86.

Hoffman, B. (1998). *Inside Terrorism*. London.

IMO (1986). *Measures to prevent unlawful acts against passengers and crews on board ships. MSC/Circ. 443,* 26 september 1986.

IMO (2002). *Consideration and adoption of amendments tot the International Convention for the Safety of Life at Sea, 1974. SOLAS/CONF. 5/32,* 12 december 2002.

IMO (2002). *Consideration and adoption of the International Ship and Port Facility Security (ISPS) Code. Consideration and adoption of the resolutions and recommendations and related matters. SOLAS/CONF. 5/34,* 17 december 2002.

Informatiedossier DGG (2003). *Dossier nieuwe bewindslieden versie 2,* 7 januari 2003.

Jaarverslag KVNR (2001). *Vaart houden.*

Lindblom, C.E. (1964). The Science of Muddling Through, in: Gore, W.J. & Dyson, J.W. *Public Administration Review*. London, John Wiley.

March, J.G. en Simon, H.A. (1958). *Organizations*. New York, John Wiley.

Nederlandse Ambassade te Washington (2002). *De Verenigde Staten nader belicht. Situatieschets 32,* 20 november 2002.

Nudell, M. en Antokol, N. (1988). *The Handbook for Effective Emergency and Crisis Management.* Massachusetts/Toronto, Lexington Books.

Overdrachtsdossier DGG (2003). *Dossier nieuwe bewindslieden versie 2,* 7 januari 2003.

Perrow, C. (1984). *Normal Accidents. Living with high-risk technologies.* USA, BasicBooks.

Price, W. (2004). Reducing the Risk of Terror Events at Seaports, in: *Review of Policy Research, Volume 21, Number 3.* Malden, USA, Blackwell Publishing. pp. 329-349.

Rosenthal, U. (1984). *Rampen, rellen, gijzelingen.* Amsterdam/Dieren, De Bataafsche Leeuw.

Rosenthal, U. en ’t Hart, P. (1985). *Crisisbesluitvorming: organisaties en mensen in kritieke omstandigheden.*

Rosenthal, U. en ’t Hart, P. (1998). *Flood Response and Crisis Management in Western Europe, A Comparative Analysis.* Berlin Heidelberg New York, Springer-Verlag.

Rijkswaterstaat, Adviesdienst Verkeer en Vervoer (2001). *De infra op scherp. Infrastructuur als terroristisch wapen. Hoe kwetsbaar is Nederland (vertrouwelijk rapport),* 30 oktober 2001.

Tops, P.W., Boogers, M.J.G.J.A. & Brandsen, T. (2003). *Rampen, Regels, Richtlijnen. De status van informele regelgeving op het gebied van rampenbestrijding*. Tilburg, Centrum voor Recht, Bestuur en Informatisering.

Tweede Kamer der Staten-Generaal (vergaderjaar, 2003-2004, 27 925, nr. 110). *Bestrijding internationaal terrorisme.* Den Haag.

VNO-NCW (2003). *Als het echt fout dreigt te gaan, praktische tips voor crisismanagement in de onderneming.* April 2003.

Internetsites

Dossier Terrorisme. [http://www.kb.nl/kb/dossiers/terrorisme/terrorisme.html]. 17 januari 2003.

Department of Homeland Security. [http://www.house.gov/rules/homeland.pdf]. 12 juni 2003.

ETA. [http://proto.thinkquest.nl/~llb142/pages/terreurgroepen/eta.htm]. 17 januari 2003

IRA.[http://proto.thinkquest.nl/~llb142/pages/terreurgroepen/ira.htm]. 17 januari 2003

Bijlage 1: Respondentenlijst

Interne actoren

DCC

- Gerard Laanen
  - Hoofd DCC

DGG

Directie A

Afdeling IHI:

- Wytske van der Mei
  - Plaatsvervangend hoofd IHI

- Maarten van der Meide
  - Beleidsmedewerker Security Havens

Afdeling AIZ

- Jaco van Hekke
  - Hoofd afdeling Algemene en Internationale Zaken
  - Leider Taskforce Security DGG

Directie V

- Richard Akerboom
  - Nederlandse delegatieleider in het MSC: het Maritime Safety Committee van IMO

Directie TI

- Hans van Leuven
  - Coördinator Internationale Zaken bij afdeling TZ
  - Plaatsvervangend leider van de Taskforce Security DGG

- Henk Merkus
  - Clusterleider Arbeidsmarkt en Onderwijszaken bij afdeling TZ
  - Waarnemend hoofd afdeling TZ met in portefeuille ILO-zaken en de implementatie daarvan & ID-card van zeevarenden

HDJZ

- Tim Timmers
  - Wetgevingsjurist (HDJZ – Scheepvaart)

Externe actoren

BZK
- Arnold Poelman
  - Medewerker AIVD

BUZA
- Eric Spaans
  - Senior-beleidsadviseur Directie Economische Samenwerking/Verkeersafdeling (DES/VA)

VROM
- Bert Duyndam
  - Medewerker KernFysische Dienst (KFD). De KFD houdt toezicht op nucleaire installaties

IVW
- Andy Joosse
  - Beleidsmedewerker divisie Scheepvaart.
  - Betrokken bij het implementatietraject

- Robbert Appeldoorn
  - Kwartiermaker Expertisecentrum Security

KVNR
- Tjitso Westra
  - Beleidsmedewerker operationele zaken

HBR
- Sander Doves
  - Beleidsadviseur maritieme ontwikkelingen (strategie en coördinatie)

Deltalinqs
- Tineke de Graaf
  - Staf Milieu & Veiligheid.

Amerikaanse ambassade
- Philip Kosnett
  - “Chief, Global Issues Section”

Rederij Spliethoff
- Marco van Rijsinge
  - Medewerker “Safety, Quality, Environment”

Regiokorps Rotterdam-Rijnmond
- Henk van Unnik
  - Hoofd Inspecteur en directeur van de “Port Security Development Group”

Bijlage 2: Interviewvragen

Opmerking vooraf:
In geval van het interviewen van een interne actor, dient de benaming van “organisatie” in de vraagstelling opgevat te worden als “afdeling” dan wel een “organisatieonderdeel”, dat een belang heeft bij het onderwerp van dit afstudeeronderzoek.

1. Wat zijn volgens u de bedreigingen voor het maritieme cluster indien er sprake is van een dreiging van terrorisme, dan wel van een terroristische aanval?

2. Welke maatregelen heeft uw organisatie reeds intern doorgevoerd die de veiligheid van maritieme aangelegenheden - in brede zin - bevorderen?

3. Wat was de aanleiding dat uw organisatie dergelijke maatregelen ondernam?

4. Welke maatregelen mist u in dit kader bij andere organisaties?

5. Welke maatregelen verwacht u die uw organisatie en DGG nog moeten doorvoeren om te voldoen aan een veilig maritiem cluster?

6. Wat is de rol van uw organisatie binnen het maritieme cluster indien er sprake is van een dreiging van terrorisme, dan wel van een terroristische aanval?

7. Is er sprake van een informatie-uitwisselingsysteem met andere organisaties en in hoeverre denkt u dat uw organisatie deze informatie-uitwisseling beïnvloedt c.q. welke rol denkt u dat uw organisatie binnen het security-netwerk heeft? M.a.w. hoeveel macht en invloed denkt u dat uw organisatie heeft?

8. Welke organisatie(s) is (zijn) voor u het meest belangrijk om aan informatie over securitybeleid te komen?

9. Van welke organisatie(s) ontvangt u de meeste informatie over securitybeleid?