

Onderzoek naar de invoering van de

International Ship and Port Facility Security code

in de Rotterdamse haven



Student: Jack Lensen (268674)
Scriptiebegeleider: Dr. A. Cachet
Erasmus Universiteit Rotterdam
Faculteit der Sociale Wetenschappen, vakgroep Bestuurskunde

Augustus, 2005

Implementa'tie, v.,1.bewerktuiging; voorziening met uitvoeringsmiddelen;-2. uitvoering, vervulling van een overeenkomst, een verdrag, een plan e.d.;-3. het invoeren van een nieuw systeem in een (data) verwerkende organisatie.

In'voeren,-5. als overheid of met zijn gezag in werking doen komen:

(Van Dale, groot woordenboek der Nederlandse taal)

Voorwoord

Het bekende spreekwoord: “de laatste loodjes wegen het zwaarst” is van toepassing geweest bij het schrijven van deze scriptie. Een wetenschappelijke studie vraagt nu eenmaal om een goede afronding. Ik heb een onderwerp gevonden dat aansluit bij mijn werkomgeving en ervaring; de invoering van wetgeving op het gebied van beveiliging van de haven van Rotterdam tegen terroristische aanslagen op schepen of het gebruik van schepen voor een terroristische aanslag. Na een intensief jaar van invoering en toetsing is het goed om terug te kijken hoe de invoering onder grote tijdsdruk is verlopen. Volgens mij is de invoering succesvol geweest. In mijn scriptie zal ik een beeld scheppen van de aanleiding, de omgeving en de wijze waarop de invoering is verlopen.

Inhoudsopgave

VOORWOORD **3**

INHOUDSOPGAVE **5**

1. INLEIDING **7**

1.1	KADER	7
1.2	PROBLEEMSTELLING	8
1.3	DOELSTELLING	8
1.4	CENTRALE VRAAG	8
1.5	DEELVRAGEN	8
1.6	AFBAKENING	8
1.7	METHODOLOGIE	9
1.8	UITGANGSPUNTEN EN AANNAMES	9
1.9	LEESWIJZER	10

2. INVOERING, DE THEORIE **13**

2.1	DE BELEIDSCYCLUS	13
2.2	BEPERKINGEN BELEIDSPROCES	14
2.3	POLICY WINDOW	15
2.4	INVOERING	15
2.5	TOP-DOWN	15
2.6	BOTTOM-UP	16
2.7	SYNTHESIZERS	17
2.8	DE KUNST VAN HET INVOEREN	18
2.9	VAN THEORIE NAAR EMPIRIE	19

3. VEILIGHEID EN TERRORISME **21**

3.1	ONTWIKKELINGEN	21
3.2	VEILIGHEID	21
3.3	TERRORISME	21

4. DE ROTTERDAMSE HAVEN **25**

4.1	OMVANG VAN DE HAVEN	25
4.2	VEILIGHEID IN DE HAVEN	26
4.3	TERRORISME IN DE HAVEN	26

5. ISPS CODE	29
5.1 DE ISPS CODE	29
5.2 WETGEVING	31
5.3 OVERIGE INITIATIEVEN	33
5.4 DE ORGANISATIE	34
6. INVOEREN ISPS CODE IN ROTTERDAM	37
6.1 HET ROTTERDAMSE MODEL	37
6.2 JURIDISCHE KADERS	38
6.3 DE WERKWIJZE	39
7. HANDHAVEN IN ROTTERDAM	45
7.1 HANDHAVING IN ROTTERDAM	45
7.2 DE DRIE FASEN	46
7.3 INFORMATIE	47
8. INVOERING, EEN ANALYSE	49
8.1 OVERZICHT	49
8.2 TOP-DOWN	50
8.3 POLICY WINDOW	50
8.4 KRITIEK	51
8.5 ANTICIPEREN	53
8.6 MANAGEN	54
8.7 RELATIES	55
8.8 MACHT	57
8.9 COMPETENTIES	58
8.10 BUDGET	58
8.11 COMMUNICATIE	59
8.12 AFRONDING	59
9. HANDHAVING, EEN ANALYSE	63
9.1 HANDHAVING IN ROTTERDAM	63
9.1 MACHT	63
9.2 COMPETENTIES	64
9.3 BUDGET	64
9.4 COMMUNICATIE	64
9.5 AFRONDING	65
10. SAMENVATTING EN CONCLUSIE	67
LITERATUUROVERZICHT	75

1. Inleiding

1.1 Kader

Na de aanslagen in de Verenigde Staten van Amerika in september 2001 is er veel veranderd. Het besef dat terrorisme zich niet houdt aan landsgrenzen is steeds groter geworden. De Verenigde Staten van Amerika verklaarden zelfs de oorlog aan het terrorisme. Diverse terroristische organisaties werden aangevallen; probleem hierbij was en is dat deze organisaties niet gebonden zijn aan één land. Enkele landen geven steun aan deze groeperingen of laten hun grondgebied gebruiken als basis voor een organisatie maar zijn niet als zodanig zelf een terroristische organisatie. Resultaat is dat de Verenigde Staten van Amerika actief zijn in diverse landen verspreid over de hele wereld om het terrorisme te bestrijden.

Niet alleen in de verschillende landen draaien inlichtingendiensten op volle toeren om mogelijke informatie te verzamelen, ook binnen wereldwijd functionerende organisaties is terrorisme een 'hot item'. Zo heeft de International Maritime Organisation (IMO) een voorschrift opgesteld voor de beveiliging van schepen en havenvoorzieningen. Dit voorschrift, de International Ship and Port facility Security code (verder afgekort als ISPS code) wordt als ANNEX toegevoegd aan het SOLAS verdrag (Safety Of Life At Sea: internationale conventie voor de veiligheid van leven op zee).

De ISPS code bevordert en benadrukt een security-cultuur binnen de gehele operationele maritieme structuur, strekkend tot maritieme beveiliging op schepen en in havens. Randvoorwaarde hierbij is dat de scheepvaart ongehinderd de handelsstromen effectief en efficiënt moet kunnen blijven dienen. Om dit te kunnen waarborgen stelt de IMO dat schepen en havenvoorzieningen adequaat dienen te zijn voorbereid op de mogelijkheid van terroristische aanslagen of andere vormen van criminele voornemens. Voor 1 juli 2004 moest deze wetgeving zijn geïmplementeerd en dienden bedrijven en schepen te voldoen aan de gestelde eisen.

In navolging van de IMO heeft de Europese Unie een Verordening opgesteld, waaraan de Europese lidstaten moeten voldoen. De verordening is in feite een aanscherping van de IMO regelgeving. Wat in de IMO regelgeving als een aanbeveling wordt gedaan is in de Europese Verordening veelal als eis aangemerkt.

In Nederland is de Havenbeveiligingswet opgesteld. Deze wet regelt de bevoegdheden van het gezag en de inrichting van de structuur van de port security in Nederland. Het voornemen was om de wet met ingang van 1 juli 2004 in te voeren in Nederland.

In Rotterdam is de burgemeester de zogenaamde Designated Authority (verantwoordelijke autoriteit), dat inhoudt dat de burgemeester namens de Minister van Verkeer en Waterstaat de bedrijven, of zoals in de IMO wetgeving genoemd, de port facilities kan certificeren in gevolge de IMO regelgeving (attributie). Het besluit of al dan niet aan de eisen is voldaan is een beschikking in de zin van de Algemene wet Bestuursrecht; bezwaar en beroep is derhalve mogelijk. De burgemeester heeft de taken ten aanzien van de invoering van port security gedelegeerd aan de Havenmeester van Rotterdam. In de nieuwe Havenbeveiligingswet wordt deze taak toegekend aan een Port Security Officer (Havenbeveiligingsofficier); in Rotterdam de Havenmeester. De Havenmeester is dus verantwoordelijk voor het operationaliseren van de port security.

De bedrijven in de haven zijn verplicht om, per havenfaciliteit (port facility), een zogenaamd risk assessment (risico analyse) uit te voeren. Vervolgens dient een havenfaciliteit beveiligingsplan (port facility security plan) te worden opgesteld en ter toetsing te worden aangeboden aan een onafhankelijk Toetsingsteam. Dit Toetsingsteam beoordeelt de plannen en de fysiek genomen maatregelen om de kans op terroristische daden te verkleinen. In Rotterdam zal na beoordeling en toetsing de burgemeester al dan niet de port facility certificeren.

1.2 Probleemstelling

De (bestuurlijke) inbedding van havenbeveiliging (port security) in Rotterdam en in het algemeen in Nederland, leverde vele vragen op. Diverse partijen speelden een rol of willen nog steeds een rol spelen. Het was een mega operatie onder een grote tijdsdruk; vóór 1 juli 2004 moesten de maatregelen zijn ingevoerd en zijn getoetst. Het ging hierbij om meer dan 140 havenfaciliteiten (port facilities) in de Rotterdamse haven. Op het gebied van beveiliging (security) betekende dit een enorme inhaalslag. De belangen van de overheid en het bedrijfsleven waren en zijn, niet altijd dezelfde, zeker in dit geval. Ondernemingen zien zichzelf niet als een potentieel doel voor terroristen. Het invoeren van de beveiligingsmaatregelen kost veel geld; geld wat er niet altijd is in minder goede economische tijden. Regelmatig moesten er afwegingen worden gemaakt; proportionaliteit was daarbij een sleutelwoord. Na invoering, introductie van de nieuwe wetgeving dient handhaving plaats te vinden. Het opzetten van een handhavingsorganisatie en het uitvoeren van de handhaving kost geld. Zonder problemen wordt deze taak uitgevoerd door het Havenbedrijf Rotterdam, wat is de achterliggende gedachte?

1.3 Doelstelling

De doelstelling van mijn afstudeeropdracht is het *beschrijven en analyseren* van de wijze van de invoering van de ISPS code in de Rotterdamse haven aan de hand van de bestaande theorie en empirie. Een tweede doelstelling is het *beschrijven en analyseren* op welke wijze de handhavingsorganisatie in Rotterdam is ingericht en werkt aan de hand van de empirie.

1.4 Centrale vraag

Op welke wijze heeft introductie van de ISPS code plaatsgevonden in de Rotterdamse haven en hoe vindt handhaving plaats?

1.5 Deelvragen

1. Waarom is de ISPS code ingevoerd?
2. Wat houdt de ISPS code in?
3. Op welke wijze is de ISPS code ingevoerd?
4. Hoe is de handhaving van de ISPS code in de Rotterdamse haven ingericht?

1.6 Afbakening

Domein

De scriptie richt zich op de wijze van invoering en handhaving van de ISPS code in de Rotterdamse haven.

Tijd

De scriptie richt zich ten aanzien van de wijze van invoering op de periode voorafgaande aan de invoering, tijdens de invoering en na de invoering van de ISPS code (begin 2003 tot eind 2004). De aanbevelingen ten aanzien van de handhaving en de komende fase richten zich op de komende vier jaren.

Beperkingen

Landelijk vindt op diverse niveaus overleg plaats: er is een expert groep ingesteld, er is een landelijke overleg voor leden van het Toetsingsteam en verder zijn er diverse stuurgroepen en werkgroepen die een bijdrage leveren aan het product “port security”. Deze overlegvormen, stuurgroepen en werkgroepen zal ik niet verder bespreken. Verder gaat het in deze scriptie te ver om de verschillen in interpretatie van de wetgeving weer te geven binnen Nederland en omringende, Europese landen.

1.7 Methodologie

Keuze

Mijn onderzoek naar de invoering van de ISPS code is een kwalitatief onderzoek, gericht op het vinden van antwoorden op de vragen op welke wijze de ISPS code in Rotterdam is ingevoerd en op welke wijze de handhaving is georganiseerd. Hiertoe zal ik beschrijven en analyseren aan de hand van de theorie en empirie. Ik heb gekozen voor de titel “*Invoering* van de Internationale Ship and Port Facility Security code in de Rotterdamse haven” en niet voor “*Implementatie*” omdat de nadruk ligt op het beschrijven en analyseren van de wijze waarop de ISPS code is ingevoerd in de Rotterdamse haven. Implementatie is echter meer dan invoeren of introduceren van nieuwe wetgeving, het omvat ook de inrichting en werking van de handhaving.

Toch zou mijn scriptie niet compleet zijn als ik niet een korte beschrijving en analyse zou geven van de huidige vorm van handhaving. Hierdoor wordt het mede mogelijk om in het laatste hoofdstuk naast een samenvatting en conclusie, aanbevelingen te doen mede in het licht van wat in de komende jaren staat te gebeuren.

Literatuuronderzoek

Als eerste heb ik relevante wetenschappelijke literatuur verzameld en bestudeert over implementatie, beleidsanalyse, terrorisme en veiligheid. Naast deze wetenschappelijke literatuur heb ik documenten verzameld over de opzet en werking van het ISPS Toetsingsteam in Rotterdam, publicaties van Ministeries over port security, wetgeving, de Algemene Inlichtingen- en Veiligheidsdienst en publicaties op het internet en in diverse kranten. Ik heb gebruik gemaakt van de gezamenlijke scriptie voor de opleiding Risicomanagement van het Toetsingsteam ISPS Rotterdam en de daarvoor gehouden interviews, gesprekken en enquête.

Gesprekken

Gesprekken heb ik gevoerd met het Hoofd van de Zeehavenpolitie Rotterdam Rijnmond (drie gesprekken), beleidsmedewerkers van het Havenbedrijf Rotterdam (twee gesprekken) en collega leden van het Toetsingsteam ISPS Rotterdam (drie gesprekken).

Eigen ervaringen

Bij het beschrijven van het proces van invoering heb ik veelvuldig gebruik gemaakt van mijn eigen ervaringen en waarnemingen als lid van het Toetsingsteam ISPS Rotterdam.

1.8 Uitgangspunten en aannames

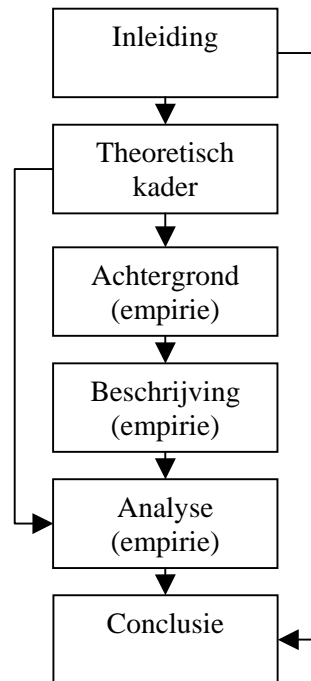
Voor dit onderzoek gelden de volgende uitgangspunten en aannames:

- Er bestaat veel literatuur en evenveel auteurs en deskundigen op het gebied van invoering van beleid, ik heb voor mijn theoretisch kader slechts gebruik gemaakt van een beperkt aantal van hen. Dat betekent niet dat ik geen waarde hecht aan al die overige theorieën.
- De gesprekken die ik heb gevoerd met het Hoofd van de Zeehavenpolitie, de beleidsmedewerkers van het Havenbedrijf Rotterdam en mijn collega's van het Toetsingsteam zijn geen gestructureerde interviews geweest. Bij onduidelijkheden tijdens het schrijven van mijn scriptie of als het gaat om vragen voor mijn beeldvorming heb ik middels directe vragen het antwoord trachten te vinden.
- Al wat ik schrijf is terug te vinden in de gebruikte literatuur zoals achter in deze scriptie is weergegeven, behalve als het gaat om mijn eigen ideeën of interpretatie. Als hier sprake van is dan zal ik dat aangeven in de tekst.
- Tijdens het schrijven van deze scriptie hebben gebeurtenissen plaatsgevonden en zijn er veranderingen in wet- en regelgeving opgetreden. Voor zover relevant heb ik die gebeurtenissen meegenomen tijdens het schrijven.
- Een volledig objectief beeld geven, als het gaat over de bijdrage en betrokkenheid van de verschillende (overheids)diensten bij de invoering van de ISPS code, is moeilijk als je als onderzoeker zelf lid bent geweest van het Toetsingsteam ISPS Rotterdam. Eigen ervaringen

kunnen het beeld hebben gekleurd. Ik heb dit zoveel mogelijk proberen te ondervangen door mijn mening te toetsen bij mijn collega's van het Toetsingsteam en een meezeer (een buitenstaander).

- De kritische vragen en opmerkingen van mijn scriptiebegeleiders hebben een bijdrage geleverd aan het expliciet maken van vaak impliciete, vanzelfsprekende ervaringen en zienswijzen.

1.9 Leeswijzer



Inleiding

In het eerste hoofdstuk leg ik uit wat het probleem is, wat mijn doelstelling is en op welke wijze ik deze doelstelling ga beschrijven. Ik leg uit welke keuzes ik moest maken en welke uitgangspunten ik heb gehanteerd bij het beschrijven en analyseren van de invoering van de ISPS code in Rotterdam.

Theoretisch kader

Het theoretische kader van invoering schets ik in hoofdstuk twee. Voordat invoering plaatsvindt is een aantal fasen in de beleidscyclus gepasseerd. Aan de hand van de door mij bestudeerde literatuur ga ik in het kort in op de onderscheiden fasen en beperkingen. Dat invoering van beleid complex is blijkt wel uit de theorie. De wijze waarop het nationale of lokale bestuur haar macht uitoefent is bepalend of invoering “top-down”, “bottom-up” of “synthesizer” wordt genoemd. De invoering van de ISPS code is een voorbeeld waarbij het bestuur de invoering afdwingt. We spreken dan van “enforcement”. Op welke wijze de invoering ook plaats vindt; kritiek op die wijze is altijd aanwezig. Wat de kritieken zijn en hoe het proces gemanaged kan worden is beschreven in hoofdstuk twee. Ik introduceer vier centrale begrippen waarlangs ik een analyse op de wijze van invoeren en op de wijze van inrichten van de handhavingsorganisatie wil uitvoeren. Deze centrale begrippen zijn: macht, competenties, budget en communicatie.

Wat niet plaatsvindt in de fase van invoering maar in de fase van agendavorming, is het gebruikmaken van een Policy window. Dat ik toch op dit onderwerp in ga heeft te maken met de relatie die er volgens mij kan bestaan tussen het op de agenda plaatsen van een onderwerp, in dit geval port security en de betrokkenheid en de rol van het Havenbedrijf Rotterdam bij de invoering van de ISPS code in Rotterdam.

Achtergrond

Het nemen van de security maatregelen, zoals vastgelegd in de ISPS code is een reactie op de aanslagen in de Verenigde Staten. Bij terroristische aanslagen staat het veroorzaken van

disproportionele angst voorop. Het doelwit is massapubliek, een bepaalde staat of de samenleving als geheel. Wat terrorisme is, welke verschijningsvormen en welke organisatievormen worden onderscheiden, beschrijf ik in hoofdstuk drie.

Het invoeren van de ISPS code in een haven als Rotterdam is omvangrijk. Vele spelers, actoren, spelen een belangrijke rol. Hoe groot de haven van Rotterdam is, wat het economische belang is, wat veiligheid betekent voor een haven, wat terrorisme betekent of kan betekenen komt aan de orde in hoofdstuk vier.

Beschrijving

De ISPS code is nieuwe wetgeving, onder druk van de Verenigde Staten ingevoerd als onderdeel van internationale wetgeving. Wat de inhoud is van deze wetgeving en welke overige wetgeving en initiatieven er zijn, zal ik bespreken in hoofdstuk vijf.

Om de ISPS code op een goede wijze in te voeren is een organisatie nodig. In Rotterdam heeft het Havenbedrijf Rotterdam van begin af aan een leidende rol gespeeld. In hoofdstuk zes beschrijf ik wie welke rol gespeeld heeft. Om de ISPS code in te voeren is een Toetsingsteam ISPS opgericht; hoe dit georganiseerd is en wat de juridische kaders zijn komen eveneens in dit hoofdstuk aan bod.

Implementeren bestaat uit invoeren en vervolgens handhaven. Het Havenbedrijf Rotterdam heeft de handhavingstaak wettelijk toebedeeld gekregen. Hoe zij deze taak uitvoeren heb ik beschreven in hoofdstuk zeven.

Analyse

De wijze waarop de invoering heeft plaatsgevonden beschrijf ik in hoofdstuk acht. Ik doe dit aan de hand van het theoretische kader en de centrale begrippen zoals ik die heb geïntroduceerd in hoofdstuk twee. De wijze waarop de invoering heeft plaatsgevonden is via de zogenaamde top-down methode. De beperkingen van deze methode zijn niet ervaren als een belemmering door de participerende diensten en de bedrijven in de Rotterdamse haven. Ik zal de wijze van anticiperen op beleid, de wijze van managen van de invoering, de relaties, de machtsposities, de competenties van de toetsingsteamleden, het budget en de vormen van communicatie analyseren.

Aan de hand van de door mij benoemde centrale begrippen zal ik de huidige wijze van handhaven analyseren. Ik doe dit in hoofdstuk negen.

Conclusie

De invoering van de ISPS code is volgens mij succesvol verlopen in de Rotterdamse haven. Succesvol omdat 125 bedrijven van de 140 bedrijven zijn gecertificeerd voor 1 juli 2004. Succesvol ook omdat geen van de bedrijven bezwaar heeft aangetekend of in beroep is gegaan. Na de invoering van de ISPS code is het zaak zorg te dragen voor handhaving en een goede beheersorganisatie. Dat met de invoering van de ISPS code het geheel van maatregelen met betrekking tot security is afgerond is een illusie. Invoering van de ISPS code was pas de eerste fase van drie fasen. Mijn doelstelling was het *beschrijven en analyseren* van de wijze van de invoering van de ISPS code in de Rotterdamse haven aan de hand van de bestaande theorie en empirie. En vervolgens het *beschrijven en analyseren* op welke wijze de handhavingsorganisatie in Rotterdam is ingericht en werkt. Desondanks kan ik het niet laten om ook enkele aanbevelingen te doen in hoofdstuk tien.

2. Invoering, de theorie

“Een Kamerlid denkt vaak dat’ie maar een motie hoeft te laten aannemen en dat dan ineens alles anders is in Nederland. Wat me ook is opgevallen is dat het kabinet zich te weinig zorgen maakt of een besluit dat we hebben genomen ook uitvoerbaar is. Je neemt een besluit, maar dan heb je wel een hele serie voetvolk nodig om dat besluit uit te voeren.”

Dit is een opmerking van de toenmalige minister Brinkman [1984] in het weekblad Vrij Nederland. Van der Graaf en Hoppe [1996] stellen dat Brinkman met deze uitspraak de spijker op zijn kop slaat. Uitvoerbaarheid van beleid is volgens hen een lange tijd een non-criterium geweest. De meeste politiek relevante actoren hebben meer belang bij woorden die goed aanslaan bij hun electoraat of achterban dan bij de daden die aan de woorden in de beleidsuitvoering zouden moeten worden verbonden. Is deze stelling ook van toepassing bij de invoering van de ISPS code in Rotterdam?

2.1 De beleidscyclus

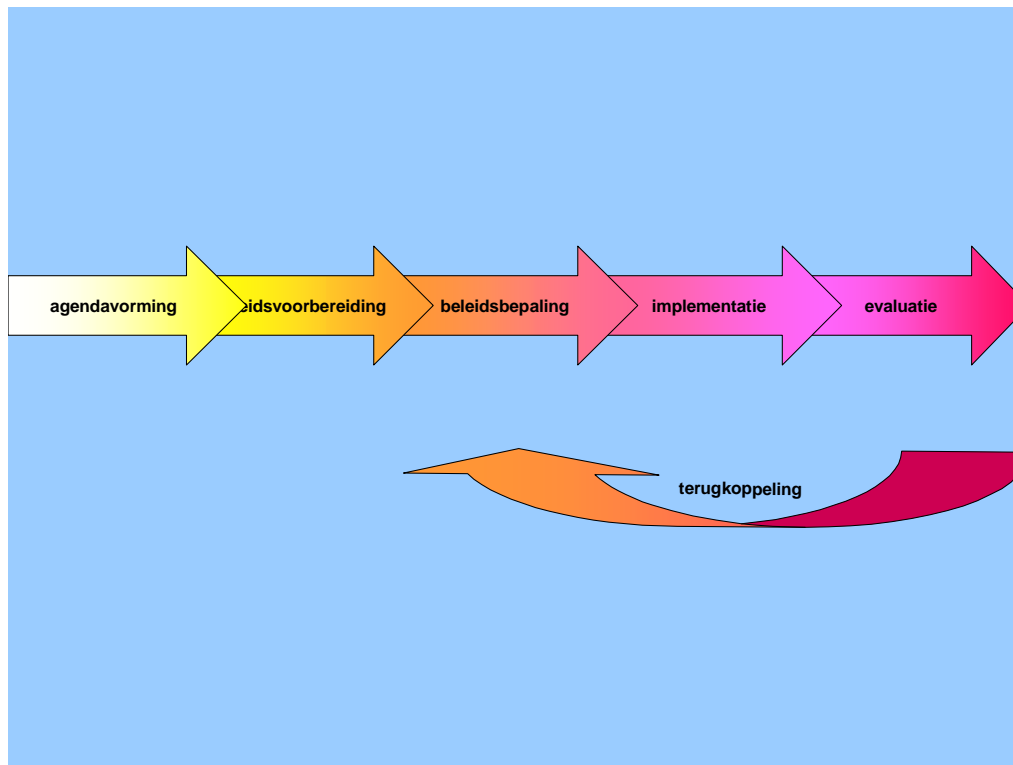
Invoering maakt deel uit van de zogenaamde beleidscyclus, ook wel het beleidsproces [Derksen, 2002] genoemd. Uitgangspunt hierbij is een bepaalde tijdsvolgorde waarin verschillende fasen plaatsvinden. In de praktijk is het zo dat fasen door elkaar heenlopen, het is niet duidelijk aan te geven op welke wijze, wanneer en onder welke invloed het proces overgaat in de volgende fase. Daarnaast is het zo dat deze fasebenadering uitgaat van een top-down model van beleid maken. Terwijl, zoals later zal blijken, veel beleid bottom-up tot stand komt.

Een veel voorkomend model is het zogenaamde fasemodel, waarbij de ene fase gevolgd gaat worden door de andere fase. Een fasemodel kan bestaan uit de volgende fasen: agendavorming, beleidsvoorbereiding, beleidsbepaling, invoering en evaluatie. Er zijn echter meerdere fasen denkbaar en inpasbaar in het model.

Een korte toelichting op de genoemde fasen:

- Agendavorming (agenda setting): welke onderwerpen komen op de politieke agenda, welke niet. Of een onderwerp op de agenda komt kan ook een gevolg zijn van een Policy window zoals eerder is aangeduid.
- Beleidsvoorbereiding (policy formulation): alternatieve oplossingen worden geschetst en vergeleken.
- Beleidsbepaling (decision making): de beslissing valt over het te voeren beleid.
- Invoering (policy implementation): invoeren en uitvoeren van het beleid.
- Evaluatie (policy evaluation): achteraf wordt bezien of het beleid de verwachte effecten of resultaten heeft gehad.
- Terugkoppeling (feedback): indien de evaluatie daartoe aanleiding geeft, aanpassing van het beleid.

De beleidscyclus:



2.2 Beperkingen beleidsproces

De harde overgang (caesuur) tussen de ene fase en de andere fase bestaat slechts op papier. Met name bij de caesuur tussen beleidsbepaling en invoering doen zich complicaties voor [Van de Graaf en Hoppe, 1996]. Niet is altijd duidelijk te maken welk beleid-als-vastgesteld dient te worden geïmplementeerd (formele caesuur). Getwijfeld kan er dan worden aan de rechtvaardigheid. Soms moet er, over delen, van het beleid nog een besluit worden genomen (voortijdige invoering van een beleidselement). Er wordt dan toch met de invoering begonnen, men handelt als het ware of er al een besluit is genomen. Dit is aan de orde als er een grote tijdsdruk rust op het invoeren van het nieuwe beleid, gesproken wordt er dan van anticiperend en / of pseudo-besluit. Het komt zelfs voor dat, delen van, het beleid al worden uitgevoerd terwijl het beleid nog niet is vastgesteld (voortijdige toepassing van een beleidselement), hier is dan sprake van anticiperende en / of pseudo-beleids-toepassing. Een veel gebruikte uitspraak is hier: nood breekt wetten.

Er zijn bezwaren tegen de hierboven genoemde complicaties. Moeten de voortijdige invoering of voortijdige toepassing worden tegen gegaan? Omdat beleid uit meerdere beleidselementen bestaat is het mogelijk een deel af te zonderen en aan de slag te gaan op de overige onderdelen. De overheid dient wel zorgvuldig te handelen en handelen, dit kan alleen op basis van een wettelijke grondslag. Omdat er sprake is van anticiperend handelen op onderdelen is het slechts een lichte complicatie. Het wordt anders als er anticiperend wordt gehandeld op (alle) wezenlijke elementen. Als het beleid (of wet) op alle fronten wordt aangepast en de anticipatie was dus niet juist dan kan dit gevolgen hebben. Er is dan mogelijk geïnvesteerd (tijd en geld) of verwachtingen gewekt of zelfs besluiten genomen. Terugdraaien is dan moeilijk. Veel wordt hier bepaald door de beleidsuitvoerenden en hun betrokkenheid bij het onderwerp.

2.3 Policy window

Deze scriptie gaat over de implementatiefase en niet over de fase van agendavorming waar de theorie van een Policy window thuishoort. Toch is het volgens mij van belang om te zien hoe snel invoering van wetgeving kan verlopen.

Kingdon schrijft in zijn boek dat een Policy window zich opent als reactie op een incident. Als een Policy window zich opent, is het gedurende een korte tijd mogelijk om radicale of ingrijpende voorstellen voor nieuwe wetgeving te doen en deze te invoeren. Beleidsmakers moeten in feite al nieuwe wetgeving hebben klaarliggen om zo snel mogelijk te kunnen reageren als deze mogelijkheid zich voordoet.

In de VS was nieuwe wetgeving snel voorhanden na de aanslagen van 11 september. Dit was, mogelijk, een reactie op het rapport van de commissie U.S. Commission on National Security / 21st Century. In februari 2001 had deze commissie in haar eindrapport "Road Map for National Security: Imperative for Change" al gewaarschuwd voor terroristische aanslagen van buitenaf in de VS. Invoering van internationale wetgeving zou volgens de VS te lang gaan duren. De sense of urgency en het feit dat een Policy window maar een beperkte tijd open staat dwongen de VS te zoeken naar een manier om snel een wijze van invoering te vinden. De aanslagen hebben zeker bijgedragen aan het besef dat er maatregelen moesten worden genomen; de VS waren zelf een doelwit geworden. De oplossing, ten aanzien van zeescheepvaart werd gevonden in het aanpassen van het SOLAS verdrag waardoor vele landen direct werden gebonden.

2.4 Invoering

"Invoering van beleid is complex". Dit zijn de woorden van Hill en Hupe in het laatste hoofdstuk van hun boek "Implementing Public Policy" [2002]. Hill en Hupe categoriseren onderzoekers naar de wijze waarop zij onderzoek hebben verricht naar implementaties van nieuw of bestaand beleid. Zij onderscheiden drie perspectieven van waaruit onderzoek kan plaatsvinden: top-down, bottom-up en synthesizers. De drie genoemde perspectieven zal ik in de komende paragrafen bespreken.

Hill en Hupe concluderen *dat de wijze waarop we kijken naar het proces van invoering wordt bepaald door: wie we zijn, wie we willen beïnvloeden en wie ons betaalt voor ons werk.*

2.5 Top-down

Het geschetste model van het beleidsproces gaat er van uit dat elke volgende stap in het proces start wanneer de voorgaande stap is afgerond. Uitgangspunt is dat beleid wordt gemaakt door "de top", met advies van de beleidsadviseurs. Dit is een vrij rationele benadering. Het behalen van de vooraf gestelde doelen staat dan ook voorop. Het gaat hierbij om zowel het te bereiken resultaat en het te bereiken effect (output en outcome).

Invoering is het product van wat in een eerder stadium van het beleidsproces is besloten, of zoals Hill en Hupe zeggen *"implementation follows formulation and decision theorem"*.

Een hele simpele gedachte achter het top-down perspectief is dat degenen die het beleid formuleren, democratisch zijn gekozen. Wat zij aan beleid maken is eigenlijk de wens van de kiezers. Als alle benodigde middelen maar beschikbaar worden gesteld voor de invoering van het beleid dan gaat het als het ware vanzelf [Hogwood en Gunn].

Een meer realistischer gedachte over de wijze van invoeren van beleid is dat voorafgaande aan de start van een invoering er een doel dient te zijn. De wijze waarop dit doel gehaald dient te worden moet zijn gedefinieerd, er moet dus een startpunt zijn. Wordt er geen actie ondernomen of beleid gemaakt dan zal er ook geen invoering plaatsvinden. Zo dient er ook een eindpunt te zijn, het is anders niet

mogelijk om te kijken of de invoering is geslaagd of mislukt. Kortom, beleid wordt bepaald, doelen gesteld en invoering vindt plaats [Pressman en Wildavsky, 1984].

Het slagingspercentage van de invoering wordt beïnvloed door het aantal door te voeren veranderingen en de mate van consensus over het te invoeren beleid. Hoe minder veranderingen er dienen te worden doorgevoerd en hoe hoger de mate van consensus is, hoe groter het slagingspercentage [Van Meter en Van Horn]. Er blijft echter sprake van éénrichtingsverkeer, maar rekeninghoudend met de omgeving.

Een andere insteek is dat succesvolle invoering alleen kan geschieden als alle stappen in een “game” volledig zijn doorlopen [Bardach]. Invoering van beleid dient te worden gezien als het ontwikkelen van “games”. Invoering kan daarna gebeuren aan de hand van de (vele) ontwikkelde scenario’s. Uitgangspunt van invoering van beleid is dat door “fixing the game” de problemen worden opgelost.

Zonder feedback kan er in principe geen nieuw beleid of aanvullend beleid worden gemaakt. Bekend moet zijn waarom het gestelde doel niet is gehaald, of juist wel. De relatie tussen het gestelde doel van het te invoeren beleid en ander, bestaand of te invoeren beleid is hierbij ook van belang. Consistentie tussen degenen die invoeren, de doelgroep en het opgestelde beleid [Sabatier en Mazmanian] vormt eveneens een belangrijke schakel.

Kritiek op de top-down benadering is er volop. Hill geeft in zijn boek “The Public Policy Process” [2005] aan dat invoeringstudies complex zijn omdat invoering niet alleen tot stand komt door beleid op te leggen. Invoering van beleid is vaak een vervolg op al bestaand beleid. Er wordt geen nieuw beleid gemaakt. Het succes van invoering is (vaak) afhankelijk van de gestelde doelen.

Kritiek op deze benadering wordt door Hill onderscheiden in drie vormen: kritiek op de aard van het beleid, kritiek op het onderlinge verband tussen beleidsformulering en het invoeringproces en kritiek op de normatieve uitgangspunten. Het is van belang om te realiseren dat beleid om diverse redenen wordt gemaakt: het kan internationale wetgeving zijn dat moet worden uitgewerkt, het kunnen verordeningen van de EU zijn, het kan nieuw beleid zijn omdat bestaand beleid niet werkt of verouderd is, bestaand beleid in strijd is met overig beleid, etc..

Beleid wordt niet uitgevoerd in een wereld die slechts verandering ondergaat door de uitvoering van dit ene beleid, zo stellen Van de Graaf en Hoppe [1996], een beleidsveld wordt juist gekenmerkt door vele processen van beleidsuitvoering die er tegelijkertijd op inwerken. Er zijn doelgroepen met elk hun eigen wensen en plannen ten aanzien van de verandering in het betreffende beleidsveld. Niet conforme uitvoering van het beleid is zo bijvoorbeeld lang niet altijd te wijten aan deloyaal of op eigen gedrag gericht gedrag van de uitvoerenden. Het kan dus een gevolg zijn van het handelen van andere actoren in het beleidsveld. Het top-down perspectief verduistert het zicht op de positie en rol van andere actoren in het beleidsveld zo stelt Sabatier. Van de Graaf en Hoppe noemen nog een tweede punt van kritiek. Door juist de nadruk te leggen op conformiteit tussen beleid-als-plan en beleidsuitvoering verduistert het top-down perspectief het onderscheid tussen intelligente aanpassing van beleid en een simpele afwijking van het gestelde beleid. Actoren in het betreffende beleidsveld zijn vaak vindingrijker dan de beleidsmakers.

2.6 Bottom-up

Tegenover het top-down perspectief staat het bottom-up perspectief. Het uitgangspunt is niet langer wat er volgens het beleid-als-plan zou moeten gebeuren, maar wat er in het beleidsveld werkelijk gedaan wordt door de actoren die een rol hebben, of zich een rol aanmeten, bij de uitvoering van het beleid, aldus Van de Graaf en Hoppe. Nu wordt het beleid-als-vastgesteld gezien als een verzameling van intenties, die startpunt zijn voor een onderhandelingsproces. Bij die onderhandelingen streven de betrokkenen hun eigen belangen en prioriteiten na. Deze belangen en prioriteiten hoeven niet voor het uitvoeringsproces vast te liggen, deze kunnen in de loop van de tijd worden aangepast. Barret en Fudge omschrijven het als volgt: ... “moeilijk wordt het om een apart en in de tijd volgend

invoeringproces te identificeren dat start bij de formulering van een beleidstekst en eindigt met acties. Het is beter om invoering te beschouwen als een actie continuüm waarin interactie- en onderhandelingsprocessen plaatsvinden tussen hen die het beleid uitgevoerd willen zien en hen van wie de beleidsuitvoering afhangt”.

Bekend is vooral de theorie over “street-level bureaucracy”. Lipsky duidt hiermee aan de beleidsvrijheid die uitvoerenden nemen bij de uitvoering van het beleid. Tijdens het invoeren moet dan ook rekening worden gehouden met de invloed die de uitvoerenden hebben op zowel het beleid als ook op de mensen op wie het beleid van toepassing is. Lipsky ziet “street-level bureaucracy” als een fenomeen waar niet om heen kan worden gegaan.

Hjern, Barret en Fudge zagen de activiteiten in het invoeringproces als een gevolg van activiteiten in diverse betrokken organisaties of geledingen binnen de organisatie. Tijdens het gehele invoeringproces worden keuzes gemaakt op basis van consensus [Hjern] of op basis van compromissen [Barret en Fudge]. Als invoering wordt gezien als “iets gedaan krijgen” dan is het halen van de uitvoering belangrijker dan betrokkenheid bij de uitvoering van het beleid.

Beleid kan ook helemaal van onderaf gemaakt worden. Het bottom-up perspectief brengt dan met zich mee dat, als alle bij het beleid betrokken actoren als gelijke partners in het onderhandelingsproces worden beschouwd het ontbreekt aan een criterium om aan de handelingen van de ene actor een hogere mate van legitimiteit toe te kennen dan aan de nadere. Het is gewoon onderhandelen. Als tweede minpunt noemen Van de Graaf en Hoppe dat de mogelijkheden van de diverse actoren, op de langere termijn om het beleidsveld te beïnvloeden onvoldoende tot hun recht kunnen komen.

Street level bureaucraten hebben vaak te maken met zaken die nergens in het beleid voorkomen of zijn uitgewerkt. Zij moeten dan vooral zelf kunnen handelen. Ze zullen dit dan op hun eigen wijze doen. Bepalend voor de handelswijze hierbij van de Street level bureaucraten kan de wijze zijn waarop organisaties zijn gestructureerd. Uitvoerenden, ambtenaren werken voor het algemene belang, ze denken dat ze professionals zijn in het veld, zij doen voor hun gevoel het vuile werk. Zij staan tegenover de bedenkers van het betreffende beleid in Den Haag. Als het beleid volgens hen niet werkt zijn zij geneigd om de standaard procedures aan te passen, verder te professionaliseren, te willen reorganiseren of de leiding te wijzigen.

Beleidsmakers zien op hun beurt niet altijd in waarom het beleid niet zo wordt uitgevoerd als bedoeld, zij geven de schuld aan diegene die invoeren of uitvoeren. Zij zien niet waarom beleid soms niet duidelijk is. Het totstandgekomen beleid is vaak het gevolg van compromissen en / of verschillende uitgangspunten. Voor de street level bureaucraten is soms niet duidelijk wat nu geïmplementeerd moet worden of hoe te invoeren. Zo ontstaat het “gat” tussen hoe beleid wordt gevoerd en hoe het bedacht was. Een reactie van de beleidsmakers op het niet uitvoeren zoals bedacht is het nemen van extra maatregelen, meer “control”, of nog meer regels, dat vervolgens weer leidt tot nog meer nieuw beleid. Het gat tussen de gewenste situatie en de bestaande situatie wordt hierdoor alleen maar groter.

2.7 Synthesizers

Beleidsbepaling en invoering moeten echter worden gezien als een interactieproces, het is geen éénrichtingsverkeer. Hill en Hupe gebruiken de term “synthesizers”; onderzoekers die beide benaderingen, top-down en bottom-up, samenvoegen bij het onderzoek naar de wijze van invoeren van beleid. Beleidsuitvoering is een coproductie tussen beleidsmakers, uitvoerders en doelgroepen.

Elmore benoemt dit als “forward and backward mapping”. Beleidsontwikkeling is niet alleen een zaak van deductie van middelen en maatregelen uit beleidsdoelen (forward mapping) maar ook een zaak van inleving in het beleidsveld en de daarin aanwezige actoren om de veranderingsmogelijkheden van het beleidsveld te kunnen onderkennen (backward mapping) [Van de Graaf en Hoppe].

Elk beleid van enige significante waarde is niet het resultaat van één enkele actor [Scharpf]. Beleidsbepaling en beleidsinvoering zijn het resultaat van interactie tussen diverse actoren met

afzonderlijke belangen, doelen en strategieën. Het netwerk is belangrijk voor een geslaagde invoering, zonder gat tussen beleidsbepaling en beleidsuitvoering. Een effectieve invoering hangt vervolgens weer af van de samenwerking tussen de actoren in het netwerk.

Invoering is enerzijds het bereiken van de gestelde beleidsdoelen en anderzijds het proces van beleidsuitvoering. Bij invoering spelen verantwoordelijkheid en vertrouwen een belangrijke rol: “an implementation process is a combination of responsibility and trust....” [Lane]. Planning en control en hiërarchie (sturing) aan de ene kant en spontaniteit, leren en adaptatie van probleem oplossende technieken aan de andere kant vormen belangrijke elementen.

Beleid wordt echter gemaakt in een complexe omgeving rondom het probleem waarin interactie plaatsvindt tussen een aantal actoren. Deze actoren bevinden zich in een netwerk van onderling afhankelijke actoren. Hierbij geldt dat verschillende actoren verschillende percepties kennen van het probleem. Beleid wordt uiteindelijk gevormd in een serie van “games” in een netwerk [Kickert, Klijn en Koppenjan].

2.8 De kunst van het invoeren

Het managen van invoering vindt plaats op drie verschillende niveaus van operationele activiteiten: het managen van beleidsprocessen, het managen van de interne relaties in de organisatie en het managen van externe en interne contacten. Daarnaast is er sprake van een wijze (perspectief) van bestuur waarlangs invoering plaatsvindt. Door Hill en Hupe worden drie prescriptieve (opleggende) perspectieven van governance (wijze van besturen) onderscheiden:

- autoritair bestuur: managen door “enforcement” (afdwingen), de input staat centraal;
- onderhandelend bestuur: managen gericht op “performance” (resultaat), gericht op output, normen;
- bestuur door overtuigen: het managen van “co-production” (samenwerking), gericht op de effecten als gezamenlijk resultaat.

Hill en Hupe maken een en ander duidelijk in de volgende tabel, *prescriptive perspectives on managing implementation*:

	Prescriptive perspective management		
	Enforcement (input)	Performance (output)	Co-production (outcome)
Operationele activiteiten			
Managen van beleidsprocessen	<ul style="list-style-type: none"> • Verantwoordelijkheden expliciet maken 	<ul style="list-style-type: none"> • Creëren interfaces 	<ul style="list-style-type: none"> • Beslissingsbevoegdheid expliciet maken
Managen van de interne relaties	<ul style="list-style-type: none"> • Duidelijkheid creëren over taken en competenties • Zorgdragen voor voldoende middelen 	<ul style="list-style-type: none"> • Vergroten afstemming door contract 	<ul style="list-style-type: none"> • Realiseren samenwerkingsverbanden
Managen van externe en interne contacten	<ul style="list-style-type: none"> • Vergroten motivatie en internationaliseren • Overeenstemming over standaard werkwijzen • Leiderschap • Training on the job 	<ul style="list-style-type: none"> • Vergroten onderhouden service gerichtheid • Belonen behalen doelen 	<ul style="list-style-type: none"> • Vergroten professionaliteit • Institutionaliseren klantbetrokkenheid • Vergroten gecoördineerde serviceverlening • Account management

Invoering vindt plaats langs één van deze perspectieven van bestuur. Dit bepaalt dus of we spreken van een top down, bottom-up of synthesizers wijze van invoering van beleid. Ik zal deze definities hanteren om aan te geven op welke wijze invoering heeft plaatsgevonden. In de praktijk echter kan er sprake zijn van een “uitstapje” naar één van de andere twee perspectieven. Het kan dus mogelijk zijn dat er een mix van perspectieven ontstaat bij het invoeren van beleid.

Kenneth E. Boulding onderscheidt drie principes waar een relatie op kan zijn gebaseerd, namelijk dwang, ruil en consensus. Koppelen we deze drie vormen aan de wijzen van governance van Hill en Hupe dan hoort bij autoritair bestuur dwang, bij onderhandelend bestuur ruil en bij bestuur door overtuigen consensus.

Invoering hangt dus van een aantal zaken af zoals: op welke wijze wordt het land, het ministerie, de lokale overheid bestuurd? Waar wordt het grootste belang aan toegekend, input zijde, output zijde of de effecten die behaald moeten worden met het beoogde beleid? Congruentie van de mogelijke alternatieven is belangrijk, zonder congruentie kunnen er vele problemen ontstaan, uiteraard afhankelijk van het onderwerp. Governance, de wijze van bestuur is daarbij bepalend. Non congruentie kan voorkomen. Dit leidt in de praktijk uiteindelijk tot kleine of grote problemen.

2.9 Van theorie naar empirie

In dit hoofdstuk heb ik drie perspectieven besproken waarop onderzoek wordt gedaan naar de wijze van invoeren van beleid. Bij de top-down benadering wordt het beleid volledig door de top vastgesteld. De beleidscyclus wordt stap voor stap doorlopen. De top blijft als het ware volledige controle houden over het proces. Hier tegenover staat de bottom-up benadering. Uitgangspunt hierbij is dat het beleid, mede, gemaakt wordt door de uitvoerenden. Hierbij ontbreekt de directe controle van de top op het proces maar staat het onderhandelen om de eigen doelstellingen te realiseren voorop. Als derde benadering worden genoemd de zogenaamde synthesizers, de middenweg. Beleidsuitvoering is dan een coproductie tussen beleidsmakers, uitvoerders en doelgroepleden. De wijze waarop het bestuur haar macht uitoefent is bepalend of invoering “top-down”, “bottom-up” of “synthesizer” wordt genoemd.

In de Rotterdamse situatie is bij de invoering van de ISPS code sprake van autoritair bestuur: managen door “enforcement” (afdwingen), een top-down benadering.

In de empirie en vervolgens in mijn analyse van de wijze waarop invoering heeft plaatsgevonden zal ik ingaan of er sprake was van een Policy window. Vervolgens zal ik ingaan op de door Hill genoemde minpunten van de top-down benadering:

- 1) kritiek op de aard van het beleid,
- 2) kritiek op het onderlinge verband tussen beleidsformulering en het invoeringproces en
- 3) kritiek op de normatieve uitgangspunten.

Het managen van invoering kan plaatsvinden op drie verschillende niveaus van operationele activiteiten: het managen van beleidsprocessen, het managen van de interne relaties in de organisatie en het managen van externe en interne contacten. Dit zet ik af tegen drie vormen van bestuur: autoritair (enforcement), overtuigen (co-production) en onderhandelen (performance).

Ik zal antwoord geven op de vraag of en in hoeverre er sprake was van anticiperen op komend beleid en of er sprake was van anticiperende beleidstoepassing bij de invoering van de ISPS code in de Rotterdamse haven. De invoering van de ISPS code moest snel gebeuren omdat hogere wetgeving, IMO, in december 2002 tot stand gekomen was en de deadline van inwerkingtreden gesteld was op 1 juli 2004. Europese en nationale wetgeving waren nog niet klaar toen met de invoering werd begonnen in de Rotterdamse haven. Er werden zelfs al certificaten uitgegeven aan de eerste bedrijven die voldeden aan de eisen van de ISPS code voordat de Havenbeveiligingswet in werking was getreden. Wat zijn de, mogelijke, bezwaren van voortijdige invoering of voortijdige toepassing van de ISPS code?

Een ander onderwerp wat ik zal beschrijven en analyseren zijn relaties, de horizontale en verticale relaties tussen betrokken actoren. Zij kunnen ieder een eigen belang hebben. Lokaal bestuur kan andere belangen hebben dan nationaal bestuur. Ook binnen het lokale bestuur kunnen diensten of afdelingen elk hun eigen belang hebben.

In Rotterdam heeft invoering plaatsgevonden door middel van een autoritaire wijze van bestuur. Ik heb de punten waarop ik mijn analyse baseer samengevat in één tabel:

Policy window		
Kritiek op		
... aard van het beleid	... onderling verband tussen beleidsformulering en invoeringproces	... de normatieve uitgangspunten
Managen van		
... beleidsprocessen	... interne relaties	... externe en interne contacten
Anticiperen op		
... komend beleid	... beleidstoepassing	
Relaties		
... horizontaal	... verticaal	

Mijn analyse wil ik verder baseren op een aantal centrale begrippen, die een grote rol spelen bij de invoering van nieuw beleid:

- 1) Machtspositie, macht wordt ontleend aan wetgeving (formele macht) of aan eerder verworven bevoegdheden (informele macht). Zonder formele macht, geen bevoegdheden.
- 2) Competenties, zonder kennis van zaken is het niet mogelijk een oordeel te geven over de mogelijke risico's en inrichting en werking van security maatregelen. Actoren dienen de benodigde competentie te bezitten of te verkrijgen.
- 3) Budget, het kunnen beschikken over financiële middelen is een voorwaarde om een dergelijk groot project van invoeren of handhaven te kunnen volbrengen.
- 4) Communicatie, zonder communicatie vaart niemand een juiste koers, vooral in een haven als Rotterdam niet.

Deze vier begrippen zal ik eveneens gebruiken bij mijn analyse van de opzet en werking van de handhavingsorganisatie.

3. Veiligheid en terrorisme

3.1 Ontwikkelingen

Na de aanslagen in New York, Washington DC en Pennsylvania (september 2001), in Madrid (maart 2004) en Londen (juli 2005) zijn de Westerse landen zich meer dan ooit bewust geworden van de mogelijke gevolgen van terroristische activiteiten. Het raakt nu ook de Westerse wereld en niet alleen meer de landen ver bij ons vandaan. Als reactie op de aanslagen zijn wereldwijd verdragen gesloten of afspraken gemaakt tot bestrijding van het terrorisme. Door de loyale opstelling in de oorlog tegen Irak is Nederland een potentieel doelwit geworden van terroristische organisaties. De haven van Rotterdam heeft bijvoorbeeld als doorvoerhaven gefunctioneerd voor Amerikaans legermateriaal afkomstig uit Duitsland. Een aanslag op dit logistieke knooppunt kan grote gevolgen hebben.

Na de terreuraanslagen zijn, onder meer vanuit de landelijke inlichtingendiensten, regelmatig signalen geweest van een verhoogd risico met betrekking tot de dreiging op westerse doelen. Daarbij is ook sprake geweest van nautische objecten. Er is een concrete waarschuwing geweest met betrekking tot een mogelijke aanslag op een ferrydienst in Rotterdam. Ook in de media werd in publicaties veelvuldig gespeculeerd op de risico's van de Rotterdamse haven.

Naast de legale vervoerstromen en activiteiten zullen in elke haven altijd illegale of criminele activiteiten zijn. In het Criminaliteitsbeeld van de Rotterdamse haven [2002] wordt geschreven dat zware en georganiseerde criminaliteit reeds gebruik maakt van de faciliteiten van de Rotterdamse haven. Het gaat daarbij om diverse vormen van criminaliteit, zonder terrorisme daarbij direct als misdrijf te vermelden. Men legt onder meer de nadruk op vermogensdelicten, milieudelicten en illegale in- en doorvoer van goederen alsmede personen (smokkel). Wel vermeldt men dat na de aanslagen nog meer aandacht is gekomen voor veiligheid en de mogelijkheid die de haven biedt voor terroristische groeperingen. Er wordt niet vermeld of daarbij gedacht is aan het faciliteren van de activiteiten of een mogelijke actie in de Rotterdamse haven.

3.2 Veiligheid

Wie in het groot woordenboek der Nederlandse taal van Van Dale de betekenis opzoekt van het woord veiligheid treft de volgende definitie aan: “veilige staat, toestand van iemand die of iets dat veilig is”. In de Engelse taal kennen we twee woorden die een vertaling geven voor veiligheid: safety en security. In deze scriptie is veiligheid vergelijkbaar met security: het beschermen van de burger tegen de andere burger (afgeleid van het Latijnse begrip “securitas”). Peper schets in zijn bijdrage aan de bundel “Veiligheid, studies over inhoud, organisatie en maatregelen” [2004] het beeld dat de traditionele veiligheid in een land (interne veiligheid) en de bedreigingen van buiten (externe veiligheid) door elkaar beginnen te lopen. De vijand, in dit geval de terroristen zijn overal en nergens. Netwerken of cellen komen we overal tegen. De burgers voelen zich onveiliger, worden angstig en vermijden tal van risico's. Veiligheid is in zijn ogen een schaars goed geworden.

3.3 Terrorismisme

In februari 2001 heeft de commissie U.S. Commission on National Security / 21st Century een rapport uitgebracht met analyses over de ontwikkeling met betrekking tot veiligheid in de komende 25 jaren voor Amerika. Deze commissie waarschuwde al voor terrorisme met een massale hoeveelheid aan slachtoffers gericht tegen de Verenigde Staten van Amerika (VS) op eigen grondgebied. Na 11 september is het duidelijk geworden: interne en externe veiligheid lopen door elkaar heen. Terrorismisme brengt de veiligheid van een land en haar burgers in gevaar.

In deze scriptie wordt veelvuldig gebruik gemaakt van het begrip terrorisme, er zijn vele definities voor dit begrip. Ik hanteer de definitie van de Algemene Inlichtingen en Veiligheidsdienst (verder afgekort als AIVD) [2001]:

“Terrorisme is het plegen van of dreigen met op mensenlevens gericht geweld, met als doel maatschappelijke veranderingen te bewerkstelligen of politieke besluitvorming te beïnvloeden”.

In het boek “Trends in terrorisme” [2003] geven Muller, Spaaij en Ruitenberg een overzicht van de verschijningsvormen, organisatievormen en financieringsvormen van terrorisme. Ik wil hier kort ingaan op hetgeen zij beschrijven.

Als verschijningsvormen onderkennen Muller, Spaaij en Ruitenberg: politiek-geografisch terrorisme, politiek-ideologisch terrorisme en politiek-religieus terrorisme.

Het politiek-geografisch terrorisme richt zich voornamelijk op het stichten van een eigen, onafhankelijke staat. Groeperingen zoals de ETA, de PLO en de IRA zijn hiervan bekende voorbeelden. Het politiek-ideologisch terrorisme is gebaseerd op de ideologie van een groepering. Wij kennen in Nederland het links extremisme, rechts extremisme en de zogenaamde single issues. Voorbeelden van het laatste type zijn: milieugroeperingen, anti-abortus, dierenrechten en anti-globalisme. De derde verschijningsvorm van terrorisme is het politiek-religieus terrorisme. Na de aanslagen van 11 september 2001 in Amerika, zo stellen Muller, Spaaij en Ruitenberg, wordt het politiek-religieus terrorisme gelijk gesteld aan islamitisch radicalisme maar merken daarbij op dat religieus fanatisme ook uit een andere hoek kan komen. Binnen deze vorm van terrorisme worden twee vormen onderscheiden: het religieus sektarisme en religieus fundamentalisme. Aan het religieus sektarisme ligt een radicale en nihilistische filosofie ten grondslag. Een bekend voorbeeld hiervan is de Japanse Aumsekte. Deze sekte meende dat het einde van de wereld nabij was en investeerde in chemische wapens om dit einde te bespoedigen. De religie als grondslag voor terrorisme is de laatste jaren sterk toegenomen: religieus fundamentalisme. Al snel spreken wij van islamitisch fundamentalisme of islamitisch terrorisme omdat dit voor ons de bekendste vorm is. De doelwitten van aanslagen door islamitische fundamentalisten hebben een grote symbolische waarde. Het meest bekende voorbeeld is de aanslag op het WTC in VS, september 2001.

In het boek: “Trends in terrorisme” worden drie organisatievormen van terrorisme genoemd: de traditionele hiërarchische geleide organisaties, losse netwerken (of te wel cellen) en mengvormen. De PLO is een voorbeeld van een traditioneel hiërarchisch geleide organisatie, overigens met vele kleine vertakkingen en groeperingen. Als moderne vorm wordt het fijnmazige netwerk genoemd. Het bekendste netwerk is Al Qaida. Met name de technologische ontwikkelingen zorgen ervoor dat de losse netwerken op een relatief eenvoudige wijze met elkaar kunnen communiceren.

Financiering van terrorisme gebeurt door o.a. sponsorstaten, donaties en legitieme organisaties. Ook door criminele activiteiten weten de terroristische organisaties aan financiële middelen te komen. Voorbeelden van criminele activiteiten zijn: (mensen) smokkel, fraude, wapenhandel, handel in drugs, corruptie, afpersing en ontvoering.

Volgens het jaarverslag 2003 van de AIVD [2004] heeft de strijd van islamitische terroristen tegen het Westen een aanhoudend karakter gekregen. De in de ogen van terroristen geslaagde aanslagen, zoals in Madrid (maart 2004), kunnen voor de terroristische netwerken mogelijk aanleiding zijn de ambities verder te verhogen. De AIVD constateert in het jaarverslag 2003 dat terroristische netwerken zich in toenemende mate richten op 'soft targets', personen of objecten die een gemakkelijk doelwit vormen. De netwerken hebben hun organisatorisch zwaartepunt verlegd naar semi-autonome lokale cellen, die in belangrijke mate zelfvoorzienend zijn. De netwerken zijn daardoor lastiger dan in het verleden bloot te leggen en onschadelijk te maken. De AIVD noemt de dreiging van het islamitisch terrorisme - ook voor Nederland - nog altijd aanzienlijk. In Nederland richten de netwerken zich vooral op het rekruteren van jongeren voor de Jihad en op het faciliteren van de gewapende strijd door middel van valse papieren, verblijfplaatsen en dergelijke.

In juli 2004 werd in de media volop gespeculeerd over mogelijke terreurdreigingen. Volgens een aantal landelijke dagbladen zou er op 9 juli 2004 een terreuralarm zijn afgekondigd. In ‘De Telegraaf’

van 10 juli 2004 werd gesproken over een verhoogde dreiging van aanslagen. Als doelwitten werden overheidsgebouwen en economische doelen genoemd.

Bij terroristische aanslagen staat het veroorzaken van disproportionele angst voorop. Het echte doelwit is niet het slachtoffer maar een massapubliek, een bepaalde staat of de samenleving als geheel. Enkele mogelijke doelwitten in Nederland: industriële complexen; chemie sector; tunnels; luchthavens; metro's; stadions; stedelijke centra en winkelcentra.

Zoals ik later zal beschrijven is de invoering van de ISPS code snel verlopen. In Amerika heeft men kans gezien om nieuwe wetgeving op een snelle en efficiënte wijze via al bestaande internationale wetgeving "te lanceren". Ik wil hier in het kort ingaan op het begrip "Policy windows" van John W. Kingdon [2003] in relatie tot het rapport van de commissie U.S. Commission on National Security / 21st Century. In februari 2001 had deze commissie in haar eindrapport: "Road Map for National Security: Imperative for Change" gewaarschuwd voor terroristische aanslagen van buitenaf in Amerika en voor het niet gezamenlijk functioneren van de diverse overheidsdiensten: FBI, CIA, NSA, Customs, etc. In zijn boek schrijft Kingdon dat een Policy window zich kan openen als reactie op een machtswisseling van President of autoriteit (regering) of als gevolg van een incident of ramp. Als een Policy window zich opent is het gedurende een korte tijd mogelijk om gebruik te maken van het doen van voorstellen voor nieuwe wetgeving. Beleidsmakers moeten dan in feite al nieuwe wetgeving klaar hebben liggen om zo snel te kunnen reageren. Het lijkt erop dat in Amerika de nieuwe wetgeving klaar lag, maar nog niet hoog op de politieke agenda stond. Het moment van op de agenda plaatsen was toen de aanslagen op 11 september plaatsvonden. Binnen de kortste keren was nieuwe wetgeving voorhanden en werden ingrijpende organisatorische maatregelen getroffen. Zo werd een nieuw departement, Homeland Security, met bijbehorende minister opgericht. De samenwerking en informatie uitwisseling tussen de diverse overheidsdiensten moesten worden verstevigd.

In Nederland zijn recent diverse rapporten over het functioneren van en samenwerken tussen de diverse overheidsdiensten verschenen. Waren de aanslagen een mogelijkheid om ook in Nederland "orde op zaken te stellen"? Er is in 2001 een Nationaal Actieplan Terrorisme en Veiligheid opgesteld. Eén van de punten was dat er een Nationaal Coördinator Terrorismebestrijding moest komen. De bevoegdheden en verantwoordelijkheden lagen te verspreid over de verantwoordelijke ministers van Binnenlandse Zaken en Justitie. In Nederland werd het Policy window, wederom, geopend na de aanslagen in Madrid (2004). Duidelijk werd toen dat terrorisme ook in Europa op grote schaal kan voorkomen. Hoe in de Rotterdamse haven gebruik is gemaakt van dit Policy window komt in een volgend hoofdstuk aan bod.

4. De Rotterdamse haven

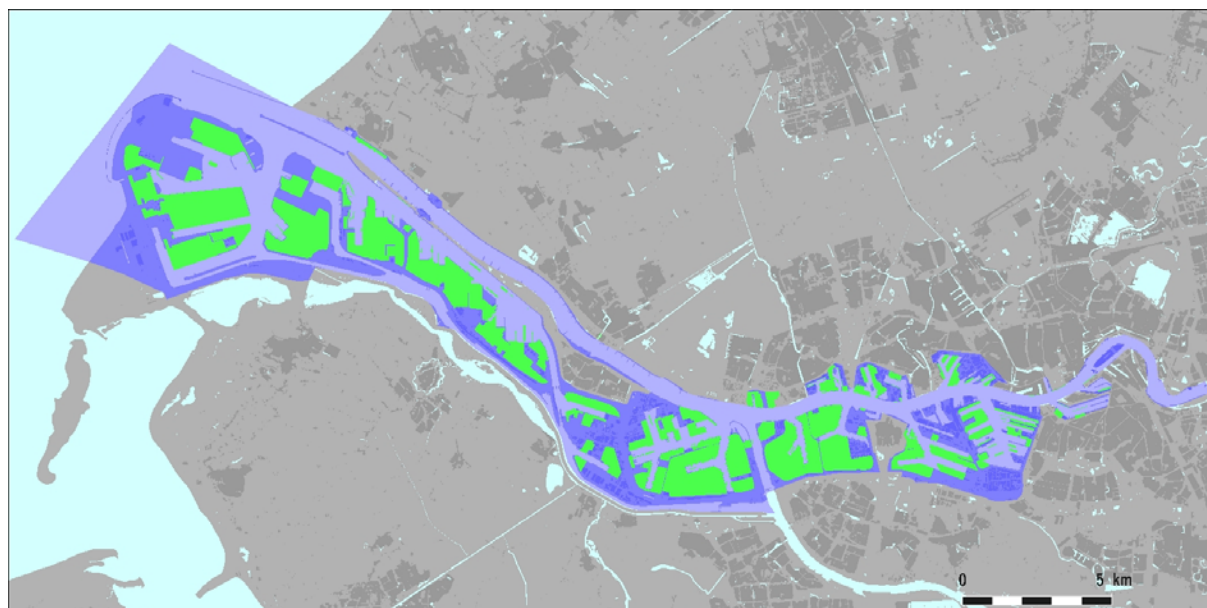
4.1 Omvang van de haven

Het Rotterdamse havengebied heeft een totale lengte van een ruim 40 kilometer. Globaal loopt dit gebied vanaf de Noordzee tot de oostelijke gemeentegrens van Rotterdam. Binnen het gebied zijn circa 400 grote en kleine bedrijven gevestigd die direct betrokken zijn bij de haven en industriesector. Indirect is het aantal bedrijven een veelvoud hiervan. De oppervlakte van de haven bedraagt 10.500 hectare, de oppervlakte van de bedrijfsterreinen 5.040 hectare en de oppervlakte van het water 3.500 hectare.

In de Rotterdamse haven werd in 2003 [Haven in cijfers 2003, 2004] in totaal 328.000.000 ton aan goederen en producten overgeslagen. Dit proces biedt een directe werkgelegenheid aan ruim 58.000 mensen. Het aandeel in het Bruto Nationaal Product bedroeg 1,5%. De Rotterdamse haven ontvangt per jaar circa 30.000 zeeschepen met jaarlijks circa 450.000 bemanningsleden en passagiers afkomstig uit alle delen van de wereld. Tevens maken circa 120.000 binnenvaartschepen gebruik van de haven. Veel bedrijven hebben een Nederlands karakter, maar in een groot aantal gevallen zijn zij volledig in buitenlandse handen waarvan de hoofdkantoren elders in de wereld staan. Hieronder zijn zowel bedrijven uit Amerika, Engeland, Duitsland, het Verre Oosten etc.

De omvang van de overslag in de haven neemt nog jaarlijks toe. Om te kunnen voldoen aan de vraag van haven- en industrieterreinen heeft het kabinet ingestemd met de aanleg van een tweede Maasvlakte. Na de realisatie van dit gebied zal de overslag vrijwel geheel uit de stad verdwenen zijn. De in de omgeving van het centrum gelegen havens zullen hun feitelijke bestemming geheel of gedeeltelijk verliezen en worden omgevormd tot woongebied. Een gedeelte van dit gebied blijft beschikbaar voor onder meer de binnenvaart en specifieke nautische takken.

Gelet op de rol van de Rotterdamse haven als 'Mainport' van de wereld en de 'Gateway' van Europa in een dicht bevolkte omgeving moet het aanwezige risico en de daaraan verbonden gevaren niet worden onderschat. Ook de aanwezigheid van vestigingen van Amerikaanse en Engelse bedrijven kan gezien worden als een risicofactor. Naar aanleiding van de gebeurtenissen in Amerika is er vanuit het openbaar bestuur een Multidisciplinair Continuïteitsplan 911 voor de regio Rotterdam-Rijnmond opgesteld. Hierin is een aantal mogelijke scenario's beschreven. Men houdt hierbij rekening met aanslagen op strategische doelen in de petrochemische industrie met een groot effectgebied, maar ook met de mogelijkheden om het logistieke proces langdurig te verlammen, of om op zichzelf staande objecten met een publieke functie onder controle te krijgen en te vernietigen.



Het paarse gebied op het kaartje is het havengebied van Rotterdam. De groene gebieden zijn de port facilities die onder de ISPS code vallen. Het totaal aantal port facilities in de Rotterdamse haven bedraagt 147 stuks. Voorwaarden om een ISPS plichtige havenfaciliteit zijn: havenfaciliteit waar goederen worden geladen of gelost door zeeschepen boven 500 ton (in internationale zeevaart), of waar passagiers aan boord van cruiseschepen of ferries van boord gaan.

4.2 Veiligheid in de haven

Op grond van de Europese wetgeving Seveso-II en het Besluit Risico's Zware Ongevallen 1999 (BRZO) zijn in de regio Rotterdam-Rijnmond 52 bedrijven verplicht tot het indienen van een veiligheidsrapport (VR). Het zijn bedrijven met aanzienlijke hoeveelheden gevaarlijke stoffen. Hierbij valt onderscheid te maken tussen stoffen die licht ontvlambaar, explosief of giftig zijn maar door hun aard en / of hoeveelheid maar een beperkt effect hebben op hun omgeving. In veel gevallen kunnen de gevolgen wel ernstig zijn maar blijven ze beperkt tot de directe omgeving. Er zijn echter ook stoffen die door hun aard en hoeveelheid een effect hebben op een groot deel van het havengebied, directe omgeving of ver daarbuiten. Veel zal afhangen van de tijdelijke of permanente situatie ter plaatse en atmosferische omstandigheden. Bij een incident in deze sector strekt het risico zich uit tot de mensen, eigendommen en belangen en activiteiten in het effectgebied. Steeds opnieuw blijkt weer dat een waarschijnlijk klein incident in deze sector een enorme impact heeft op zijn omgeving. Buiten mogelijke slachtoffers en directe materiële schade kunnen bedrijfsprocessen stagneren, delen van de infrastructuur worden lam gelegd of woongebieden deels worden ontruimd.

4.3 Terrorisme in de haven

De lamlegging van het logistieke proces kan een gevolg zijn, maar ook een doel op zich. Met het deels of volledig afsluiten van de haven ontstaat een knelpunt in het Europees distributie netwerk. Dit moet nog los gezien worden van het middel dat gebruikt wordt, de mogelijke slachtoffers en de directe materiële schade. Het lamleggen van de haven van Rotterdam kan voor een klein deel ondervangen worden door andere havens, maar de maatschappelijk en economisch impact is enorm.

Concrete aanwijzingen van terroristische activiteiten in de Rotterdamse haven zijn niet publiekelijk bekend, maar niet ondenkbaar. Al eerder was de haven het doelwit van een terroristische actie. Op 14 maart 1971 werd door de Palestijnse terreurorganisatie El Fatah een aanslag gepleegd op een petrochemische installatie in het Europoortgebied.

Waar kunnen terroristische aanslagen op gericht zijn? In hoofdstuk drie, Veiligheid en terrorisme heb ik een kleine opsomming gegeven van de mogelijke doelen voor terroristische aanslagen. Voor de Rotterdamse haven is een risicoanalyse gemaakt van de vitale objecten, installaties, tunnels, passagiersterminals, chemicaliën opslag, etc. Voor al deze objecten zal een beveiligingsplan moeten worden opgesteld.

Omdat terroristische activiteiten vooral gericht zullen zijn op het treffen van een massapubliek zijn de bedrijven in de petrochemische industrie een mogelijk doelwit omdat de effecten van een aanslag enorm kunnen zijn. Ook de toename van het aantal cruiseboten naar Rotterdam is een mogelijk doelwit. De komst van ms. Queen Mary 2, het grootste, Engelse vlaggenschip en andere Engelse en / of Amerikaanse cruiseschepen is een interessant doelwit voor terroristen.

Om een beeld te schetsen van de mogelijke risico's in een beperkt gebied heb ik een foto opgenomen met diverse objecten met een groot risico voor terroristische acties in de haven. Het zijn: de havenmond, containerterminal, passagiersterminal, elektriciteitscentrale, chemicaliënopslag en bewerking, chemicaliëntankers, olieopslag, pijpleidingen, spoorlijnen en woonkernen.



Duidelijk zichtbaar is dat op een relatief kleine oppervlakte een groot aantal potentiële doelwitten liggen voor terroristische aanslagen. De wetgeving vanuit ISPS is gericht op de zogenaamde port facilities waar zeeschepen aanmeren om te laden of te lossen. Een aantal mogelijke doelwitten zijn geen port facility: elektriciteitscentrale, spoor- en wegverkeer, woonkernen en de havenmond. Het is duidelijk dat de invoering van de ISPS code alleen geen garantie is voor een veilige haven.

Het uitsluiten van aanslagen door het treffen van beveiligingsmaatregelen is gewoon niet mogelijk. Voor een terrorist is alles een potentieel doelwit. De maatregelen zullen er voor zorgen dat het moeilijker wordt aanslagen te plegen op zeeschepen en haar bemanning. Door de maatregelen zal het wel zo zijn dat de gehele port facility beter wordt beveiligd. Recent is echter duidelijk geworden dat genomen maatregelen pas werken als de mensen zich bewust zijn van de mogelijke gevaren. Op het vliegveld Schiphol is er sprake van mensensmokkel of diefstal terwijl Schiphol goed wordt beveiligd. De ISPS code is, naast de te nemen fysieke maatregelen, gericht op de training van beveiligingspersoneel of personeel dat bepaalde beveiligingstaken krijgt opgedragen. Het geeft geen richtlijnen of aanwijzingen voor al het overige personeel.

De invoering van de ISPS code bracht een aantal neveneffecten, mogelijk onbedoelde effecten met zich mee. Een aantal voorbeelden: door de strengere controle op de identiteit van (nieuwe) medewerkers kwamen minder illegaal in Nederland verblijvende buitenlanders aan het werk in de haven. Er werd meer dan voorheen aangifte gedaan van het aantreffen van illegalen in de haven. Diefstal van onder andere containers en metalen vindt niet of nauwelijks meer plaats vanaf de haventerreinen, er is een verschuiving waar te nemen naar diefstallen en overvallen buiten het betreffende haventerrein.

5. ISPS code

5.1 De ISPS code

Op 12 december 2002 heeft de Diplomatieke Conferentie van de International Maritime Organization een aantal wijzigingen op het bestaande SOLAS-verdrag van 1974 aangenomen. De maatregelen zijn gericht op het geven van invulling aan beveiligingsmaatregelen in de maritieme sector. Deze aanvulling op het SOLAS – verdrag is de International Ship & Port Facility Security en is op 1 juli 2004 wereldwijd in werking getreden.

Het doel van de ISPS code wordt door de IMO [2003] als volgt omschreven:

- Het opzetten van een internationaal netwerk en samenwerkingsverband tussen deelnemende overheden, overheidsinstanties, lokale overheden en de scheeps- en havenindustrieën om beveiligingsrisico's te onderkennen, het treffen van preventieve maatregelen tegen beveiligingsincidenten in relatie tot schepen en havenvoorzieningen in gebruik bij de internationale handel.
- De rol en verantwoordelijkheden van de overheden, de scheepvaart en de havensector vast te leggen om op nationaal en internationaal niveau maritieme beveiliging te verzekeren.
- Te verzekeren dat er vroegtijdig efficiënt beveiligingsgerelateerde informatie wordt verzameld en uitgewisseld.
- Een methode voor beveiligingsonderzoeken beschikbaar te stellen, alsmede het invoeren van plannen en procedures om te reageren op te onderscheiden niveaus van onveilige situaties.
- Betrouwbaarheid te verzekeren en zekerheid te verkrijgen dat adequate en proportionele maritieme beveiligingsmaatregelen zijn getroffen.

Hierbij wordt onderscheid gemaakt tussen maatregelen voor de schepen en maatregelen voor de port facilities die deze schepen aandoen. De maatregelen werken suppletoir en kunnen eigenlijk niet los van elkaar worden gezien.

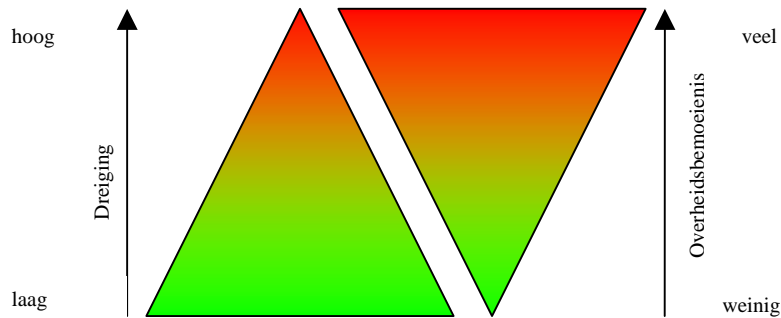
De ISPS code is van toepassing op de volgende typen van schepen die aankomen of vertrekken op internationale zee-reizen:

- passagiersschepen inclusief hoge snelheidsvaartuigen
- vrachtschepen, inclusief hoge snelheidsvaartuigen van 500 ton of meer
- mobiele off shore boorinstallaties en
- havenvoorzieningen die deze schepen bij internationale zee-reizen bedienen

De nationale overheden hebben de verplichting om er voor te zorgen dat informatie over het dreigingsbeeld beschikbaar en betrouwbaar is, risico's in kaart zijn gebracht en dat zij aanwijzingen geven bij een hoog dreigingsbeeld. Het toetsen en certificeren van de port facilities dient door of namens de nationale overheid te geschieden, inclusief het toezicht op de naleving van de beveiligingsmaatregelen.

De nationale overheid stelt op basis van het dreigingsbeeld een security level (niveau van dreiging) vast. Dit kan gebeuren op nationaal, regionaal of lokaal niveau. Hoe hoger het dreigingsbeeld hoe hoger de mate van invloed van de nationale overheid.

In een schema ziet dit er als volgt uit:



In Nederland zal het zogenaamde Nationale alerteringssysteem worden ingevoerd. Met kleuren geeft de overheid aan wat het dreigingsbeeld is. Met de invoering van de ISPS code is hier een model aan toegevoegd, de onderscheiden niveaus van beveiliging:

- Security level 1: normale omstandigheden;
- Security level 2: verhoogde dreiging;
- Security level 3: specifieke, uitzonderlijke dreiging.

Bij elk security level behoort een aantal extra beveiligingsmaatregelen als uitbreiding op het voorgaande security level. Van Gunsteren [2004] benoemt de kleuren als de mate waarin de burger bang moet zijn, hoe roder hoe banger.

Elke port facility dient een passend port facility beveiligingsplan (Port Facility Security Plan; PFSP) op te stellen, waarbij rekening wordt gehouden met de drie in de ISPS code omschreven beveiligingsniveaus. Elk afzonderlijk plan dient ten minste de volgende elementen te bevatten:

1. Maatregelen (en uitrusting) geschikt om wapens of enig ander gevaarlijk middel te ontdekken;
2. Maatregelen om ongeautoriseerde toegang tot de voorziening, afgemeerde schepen en niet toegankelijke gebieden op de port facility, te voorkomen;
3. Procedures om te reageren op veiligheidsbedreigingen of inbreuken op de beveiliging, inclusief maatregelen om van belang zijnde werkzaamheden op de voorziening het schip of de interface, gaande te houden;
4. Procedures voor evacuatie in het geval van veiligheidsbedreiging of inbreuken op de beveiliging;
5. De taken van het beveiligingspersoneel en de hen opgedragen beveiligingsverantwoordelijkheden en voor ander personeel werkzaam op de voorziening in relatie tot beveiligingsaspecten;
6. Procedures voor de samenwerking op het gebied van scheepsbeveiligingsactiviteiten;
7. Procedures voor een periodieke beschouwing van het plan en aanpassingen;
8. Procedures om beveiligingsincidenten te rapporteren;
9. De bereikbaarheid van de port facility beveiligingsofficier (Port Facility Security Officer, PFSO) of zijn vervanger(s) op 24-uurs basis;
10. Maatregelen om een effectieve beveiliging van lading en scheepsbevoorraden op de voorziening te waarborgen;
11. Maatregelen om de inhoud van het beveiligingsplan te beveiligen;
12. Maatregelen om het PFSP te herzien.

Onderwerp van beveiliging is de interface schip – port facility. De beveiligingsmaatregelen van de port facility zijn gericht op de directe omgeving waar het schip tegen de kant ligt om te laden of te lossen. Het gaat dan om de landzijde en de waterzijde. Ik zal het trachten te illustreren met een foto van het Havenbedrijf Rotterdam.



De beveiliging door de port facility is gericht op het voorkomen dat er mensen en of goederen aan boord gaan vanaf de landzijde (ship – port interface). De beveiliging van het zeeschip is erop gericht dat er geen mensen of goederen aan boord komen vanaf het schip dat langszij ligt (ship – ship interface).

5.2 Wetgeving

In de vorige paragraaf heb ik beschreven wat de inhoud en betekenis is van de ISPS code zonder diep in te gaan op alle artikelen en maatregelen. In deze paragraaf zal ik een beeld schetsen van de wettelijke kaders en relaties met andere, bestaande initiatieven. Voor deze beschrijving heb ik gebruik gemaakt van de tekst zoals die is beschreven in de scriptie Risicomanagement van de leden van het Toetsingsteam ISPS.

Op internationale wetgevingsniveau bestaat het zogenaamde SOLAS verdrag, uitgevaardigd door de IMO. In EU-verband is de juridische basis voor de regelgeving te vinden in Verordening (EG) Nr. 725/2004 van 31 maart 2004 van het Europese Parlement en de Raad betreffende de beveiliging van schepen en port facilities (hierna EU Verordening). De voornaamste doelstelling van deze Verordening is de invoering en invoering van communautaire maatregelen voor de verbetering van de beveiliging van de internationale handel en in dat kader gebruikte schepen en bijbehorende port facilities, tegen het gevaar van terrorisme. Met deze Verordening wordt de basis gelegd voor een geharmoniseerde invoering van eerdergenoemde ISPS code in EU-verband.

De EU Verordening gaat verder dan de ISPS code. Zo wordt bijvoorbeeld verplicht gesteld dat een speciale instantie in de Lidstaat (periodiek) een beoordeling van de veiligheid van de port facility uitvoert. Er worden zwaardere eisen gesteld aan de bescherming van de vertrouwelijkheid van de veiligheidsplannen en beoordelingen.

Ter invoering van de EU Verordening was voor de Nederlandse zeehavens, wegens het ontbreken van een hiertoe geëigend wettelijk kader, een nieuwe uitvoeringswet noodzakelijk. Hoewel de EU Verordening rechtstreeks in de Lidstaten werkend is moest ook nationaal nog een aantal zaken worden geregeld. De belangrijkste items zijn het aanwijzen van een Havenbeveiligingsautoriteit, de instanties

belast met de handhaving en het vereiste opleidingsniveau van beveiligingspersoneel van de port facilities.

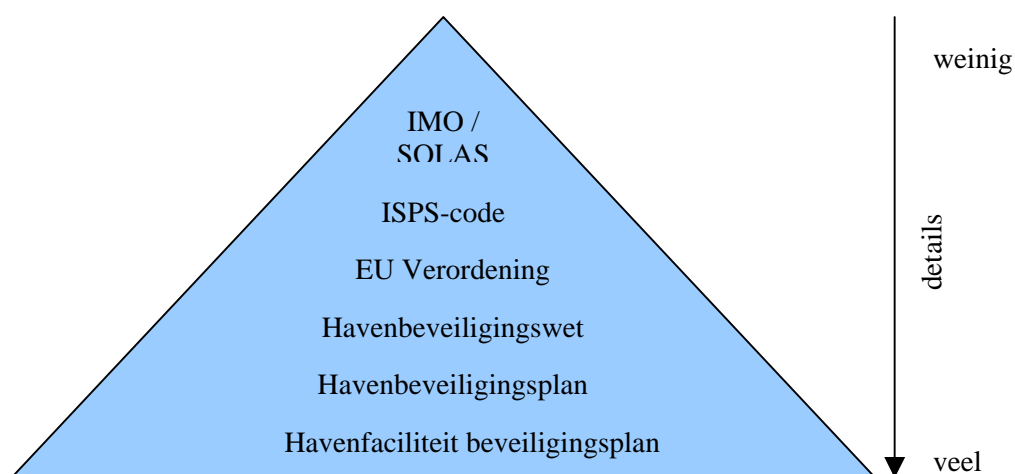
In de eerste plaats moet dus elk lid staat één of meerdere autoriteiten aanwijzen voor de maritieme beveiliging. In Nederland is in eerste instantie gekozen voor de burgemeester als Designated Authority (Havenbeveiligingsautoriteit) te benoemen. De burgemeester is primair verantwoordelijk voor de handhaving van de openbare orde en veiligheid. Verder heeft de Burgemeester, in de context van de bestuurlijke verantwoordelijkheid van het gemeentebestuur, in het bijzonder een algemene zorg voor de voorkoming van strafbare feiten die invloed hebben op de orde en rust in de gemeentelijke samenleving. De beveiligingsmaatregelen die in de Nederlandse havens zullen worden genomen, hebben een preventief karakter, die aansluiten bij de genoemde algemene zorg. Mocht er, ondanks de getroffen beveiligingsmaatregelen, toch een aanslag op een port facility worden gepleegd met ernstige gevolgen, dan is de burgemeester de bestuurder op lokaal niveau die onmiddellijk optreedt op grond van de Wet rampen en zware ongevallen. Deze spilfunctie van de burgemeester verzekert in bestuurlijk opzicht een snelle overgang van de normale situatie (veiligheidsniveau 1) via de niveaus 2 en 3 naar uiteindelijk de rampenorganisatie. Ook bij opschaling in de bestuurskolom met mogelijke overheveling naar regionaal of zelfs nationaal niveau, blijft de spilfunctie op lokaal niveau gewaarborgd door de rol van de burgemeester hierin.

In de tweede plaats dient nationaal te worden voorzien in de handhaving. Het toezicht en de verdere handhaving is middels de Havenbeveiligingswet vanuit het Rijk (de Minister van Verkeer en Waterstaat) gedecentraliseerd naar de havengemeenten. In lijn met de positionering van de toezichthoudende functie [kabinetsstandpunt op het rapport van de Ambtelijke Commissie Toezicht] is gekozen voor een eerstelijns toezicht (het rechtstreekse toezicht) op de naleving bij de havengemeenten zelf en een tweedelijns toezicht (systeemtoezicht) door de Inspectie van Verkeer en Waterstaat (IVW).

Aangezien de EU Verordening op 1 juli 2004 moest zijn geïmplementeerd is bij de behandeling van het wetsvoorstel om te komen tot de Havenbeveiligingswet zwaar ingezet op deze datum. Toen duidelijk werd dat deze datum wellicht niet gehaald zou worden heeft de Minister van Verkeer en Waterstaat een nadrukkelijk beroep gedaan op het Parlement om de behandeling van de Havenbeveiligingswet zo snel mogelijk af te ronden. Dit heeft echter niet tot het gewenste resultaat mogen leiden. De Eerste Kamer heeft op 5 juli 2004 het wetsvoorstel aanvaard en publicatie in het Staatsblad heeft uiteindelijk op 15 juli 2004 plaatsgevonden. Ondanks het feit dat de Havenbeveiligingswet in het Staatsblad is geplaatst en daarin staat aangegeven dat het een dag na plaatsing in werking treedt, is door het ministerie van Verkeer en Waterstaat bepaald dat toch nog rekening gehouden moest worden met de Tijdelijke Referendumwet (Trw). Normaliter is de Tijdelijke Referendum wet niet van toepassing op wetten die strekken tot één op één invoering van vastgestelde besluiten van de Europese Unie. Echter, de Havenbeveiligingswet strekt tevens ter invoering van toekomstige besluiten van de Europese Unie of van andere volkenrechtelijke organisaties op het gebied van de beveiliging van havens. De Havenbeveiligingswet dient derhalve niet uitsluitend tot uitvoering van een reeds vastgesteld besluit van de EU. Deze wet geeft burgers de mogelijkheid te ageren tegen nieuwe wetgeving. Dat betekent dat eenieder, binnen een periode van 6 weken, een referendum over die wet kan aanvragen. De inwerkingtreding van de Havenbeveiligingswet is op grond van de Referendumwet dan ook met 6 weken opgeschort, ongeacht wat in de Havenbeveiligingswet zelf staat ten aanzien van de inwerkingtreding. Deze termijn van 6 weken is op 9 juli 2004 ingegaan. In concreto betekent dit dat hierdoor de Havenbeveiligingswet uiteindelijk pas op 21 augustus 2004 in werking is getreden. Gevolg hiervan was dat de burgemeester niet kon optreden als Havenbeveiligingsautoriteit en kon overgaan tot de afgifte van certificaten. Om het bedrijfsleven hier niet de dupe van te laten worden hebben bedrijven die aan de eisen hadden voldaan – in afwachting van de definitieve certificering op grond van de Havenbeveiligingswet – van de Minister van Verkeer en Waterstaat een Verklaring “Beveiliging Havenfaciliteit” (Declaration of Compliance) ontvangen. Hiermee konden deze bedrijven aantonen dat zij voldeden aan de ISPS code. Deze bedrijven zijn door het ministerie van Verkeer en Waterstaat overigens ook als zodanig bij de

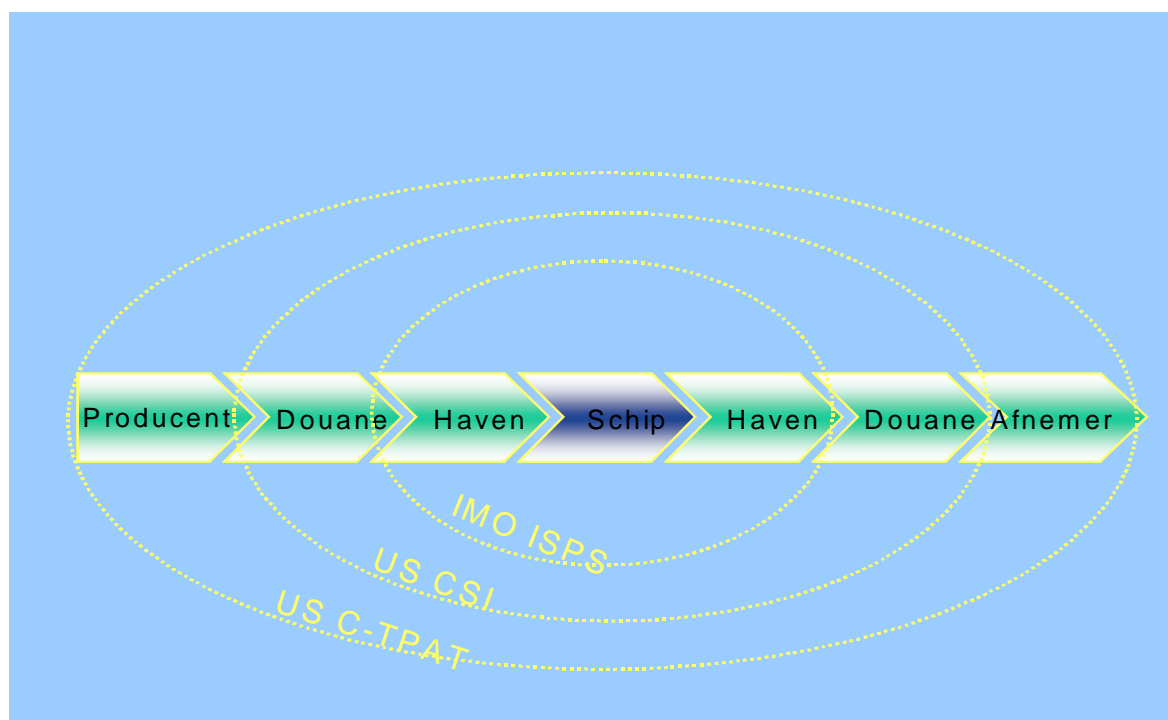
IMO aangemeld, waarna ze in het IMO Global Integrated Shipping Information System (een wereldwijd te raadplegen internetsite) zijn opgenomen.

Zet ik de wetgeving in een schema, dan ziet dit er als volgt uit:



5.3 Overige initiatieven

Zeescheepvaart is niet de enige vorm van transport dat een mogelijk doelwit kan zijn voor terroristen of waarvan gebruik kan worden gemaakt. Vanuit de VS worden meerdere initiatieven ontplooid om de beveiliging van het land te vergroten. Eén van die initiatieven is het zogenaamde C-TPAT (Customs-Trade Partnership Against Terrorism). Dit initiatief is gericht op de veiligheid van de supply chain (de keten van producent naar afnemer) naar een hoger veiligheidsniveau te brengen. De Amerikaanse douane speelt hierin een grote rol. Een tweede initiatief is het zogenaamde CSI (Container Security Initiative). De Amerikaanse douane scant op basis van risicoanalyse containers in de haven waar ze worden geladen aan boord van zeeschepen. Op diverse plaatsen in de Rotterdamse haven zijn nucleaire detectiepoorten geplaatst in samenwerking met de VS om het illegaal transporteren van nucleaire goederen te voorkomen.



Voldoen de goederen aan de eisen die de Amerikaanse overheid stelt, dan kan dit een economische voordeel opleveren, de afhandeling in de VS zal sneller verlopen dan wanneer er niet wordt voldaan aan de eisen.

C-TPAT, CSI en ISPS zijn alle drie gericht om te voorkomen dat zeeschepen en of hun goederen doelwit zijn van terroristische aanslagen. Of, een tweede mogelijkheid de zeeschepen en of hun lading als middel worden gebruikt voor aanslagen.

5.4 De organisatie

De Minister van Verkeer en Waterstaat is verantwoordelijk voor de maritieme beveiliging in Nederland. Ten aanzien van de beveiliging van port facilities en zeeschepen heeft de Minister de volgende verantwoordelijkheden:

- Het voeren van communicatie met de Internationale Maritieme Organisatie (IMO);
- Contactpunt voor Havenbeveiliging voor de Europese Commissie en andere lidstaten;
- Invoering van de ISPS Code op nationaal niveau.

De vertaling van deze verantwoordelijkheden naar beleid is uitgevoerd door het Directoraat Generaal Goederenvervoer (DGG) van het ministerie van Verkeer en Waterstaat. Om een breed draagvlak te creëren heeft het DGG de expertgroep Havenbeveiliging opgericht waarin naast het DGG ook vertegenwoordigers zitten van de grote zeehavens. Onder de verantwoordelijkheid van de expertgroep is de 'Leidraad Beveiliging Havens en Port Facilities' opgesteld. Hierin zijn beleidsrichtlijnen voor de landelijke invoering van de ISPS Code vastgesteld. Richtlijnen voor de attributie van een groot aantal verantwoordelijkheden van de nationale centrale autoriteit voor Havenbeveiliging naar de regionale Havenbeveiligingsautoriteit wordt gezien als het belangrijkste kenmerk van de Leidraad.

In de Leidraad wordt de keuze gemaakt om als regionale Havenbeveiligingsautoriteit de burgemeester aan te wijzen. Ter motivatie van deze keuze worden de volgende overwegingen gegeven:

- Er moet sprake zijn van een officiële bestuurlijke en juridische rechtspersoon of instantie;
- Er mag geen sprake zijn van een politieke constellatie (zoals het college van B&W);
- De rechtspersoon of instantie dient in een hiërarchieke relatie te staan tot politie, havenautoriteiten en hulpdiensten en zijn rol dient inpasbaar te zijn in de calamiteiten-rampenbestrijdingplannen;
- Bij de keuze dienen handhaving en sanctiemogelijkheden een punt van overweging te zijn;
- Bezwaar en Beroep dienen mogelijk te zijn.

De burgemeester van Rotterdam is door de Minister van Verkeer en Waterstaat benoemd als regionale Havenbeveiligingsautoriteit van Rotterdam Rijnmond. Hij is hiermee verantwoordelijk voor de beveiliging van de havens van Rotterdam, Schiedam en Vlaardingen. Als autoriteit heeft de burgemeester de volgende taken:

- Aanwijzen van een Havenbeveiligingsofficier (Port Security Officer; PSO);
- Het uitvoeren van een risicoanalyse voor iedere port facility;
- Het beoordelen van, door port facilities op te stellen, beveiligingsplannen;
- Het lokaal laten afkondigen van landelijk bepaalde dreigingfasen;

De Havenbeveiligingsofficier vervult een coördinerende rol in de uitvoering van havenbeveiliging. Voor het havengebied van Rotterdam, Schiedam en Vlaardingen is de (Rijks)Havenmeester van Rotterdam door de burgemeester aangewezen als Havenbeveiligingsofficier. In het Havenbeveiligingsplan (Port Security Plan) van Rotterdam wordt hiervoor de volgende motivering gegeven: "Vergelijkbaar met zijn taken binnen de nautische verantwoordelijkheden, is de Havenmeester de meest geschikte functionaris om zowel de beheerstaken als operationele taken met betrekking tot havenveiligheid vorm te geven. Veel van deze taken liggen immers in het verlengde van zijn verantwoordelijkheden en bevoegdheden als Havenmeester. Het apparaat (zowel werknemers als infrastructuur) dat de Havenmeester in zijn functie als hoofd van de Rotterdam Port Authority (RPA)

ter beschikking staat, gebruikt hij tevens om de functie van Havenbeveiligingsofficier uit te kunnen voeren.”

De burgemeester van Rotterdam kan niet op detailniveau betrokken zijn bij de beleidsontwikkeling en uitvoering van havenbeveiliging noch bij de uitvoering hiervan. De burgemeester moet als eindverantwoordelijke kunnen vertrouwen op uitgewerkte beleidsrichtlijnen van een adviesorgaan. Voor de ontwikkeling van Regionaal Havenbeveiligingsbeleid is daarom de Port Security Policy Board (PSPB) opgericht.

In Rotterdam wordt van oudsher veel samengewerkt tussen de gemeentelijke diensten, vooral op het gebied van veiligheid en milieu. De rampen in Enschede en Volendam hebben de noodzaak van een verregaande samenwerking op het gebied van rampenbestrijding nog evidentier gemaakt. De overeenkomsten tussen rampenbestrijding en terreurbestrijding zijn aanleiding geweest voor de burgemeester van Rotterdam om het onderwerp havenbeveiliging aan te laten sluiten bij de bestaande topstructuur van veiligheidsoverleg, het Regionaal Beleidsoverleg Rampenbestrijding, afgekort RegBOR. In het RegBOR Rotterdam hebben de hoofden van de volgende diensten zitting:

- Regionale Hulpverleningsdienst Rotterdam Rijnmond RHRR (voorzitter)
- DCMR Milieudienst Rijnmond
- Rotterdam Port Authority (Havenmeester)
- Openbaar Ministerie
- Douane district Rotterdam
- Bestuursdienst Rotterdam
- Politie Rotterdam Rijnmond, Zeehavenpolitie
- Port Security Officer
- Gemeentelijke Hulpverlening bij Ongevallen en Rampen (GHOR)

De politie, de Port Security Officer en de douane zijn pas deel gaan uitmaken van het RegBOR na de oprichting van het Port Security Policy Board. Het RegBOR wordt voorgezeten door de RHRR, de brandweerorganisatie van Rotterdam. Bij rampen en ongevallen heeft de RHRR een regierol dat het voorzitterschap rechtvaardigt.

De Port Security Policy Board bestaat uit de RegBOR leden, aangevuld met het hoofd van de Zeehavenpolitie en de directeur van het Havenbedrijf Rotterdam N.V..

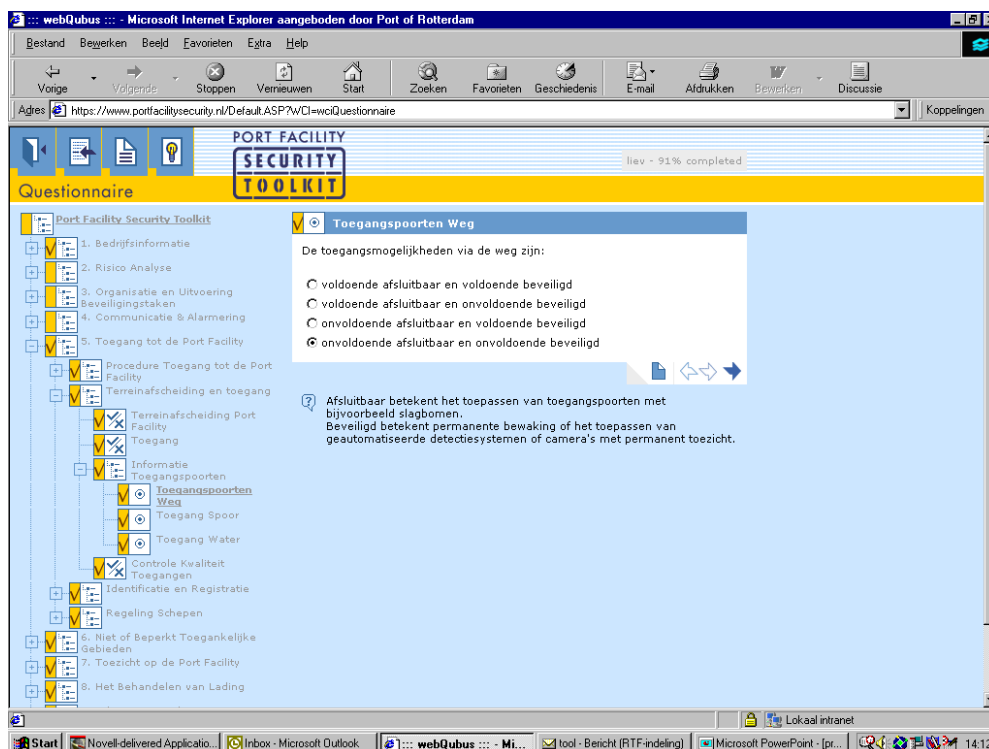
6. Invoeren ISPS code in Rotterdam

6.1 Het Rotterdamse model

Aan het begin van 2003 heeft de Port Security Policy Board de burgemeester geadviseerd over de gewenste aanpak van de invoering van de ISPS code in Rotterdam. Dit advies heeft de basis gevormd voor het 'Rotterdamse model', een plan van aanpak dat door het Ministerie van Verkeer en Waterstaat is overgenomen ten behoeve van de invoering van de ISPS code bij de andere zeehavens in Nederland. Het Rotterdamse model kende twee speerpunten:

- het bedrijfsleven wordt uitgerust met een geautomatiseerde omgeving waarin de risicoanalyse van port facilities evenals het opstellen van een beveiligingsplan mogelijk wordt gemaakt en in grote mate wordt vereenvoudigd;
- voor de beoordeling van havenfaciliteit beveiligingsplannen en de genomen maatregelen wordt een multidisciplinair Toetsingsteam opgericht.

De geautomatiseerde omgeving kreeg zijn gestalte in de zogenaamde Port Facility Security Toolkit. Met "de Toolkit" wordt aan de hand van een geautomatiseerde vragenlijst inzicht gevraagd in de beveiliging van een port facility. Ook is het mogelijk om met de Toolkit een compleet beveiligingsplan op te stellen.



De beveiligingsmaatregelen die de port facilities hebben genomen moesten door de overheid worden getoetst. Door de burgemeester van Rotterdam werd een Toetsingsteam geformeerd. De samenstelling in de Rotterdamse haven van het Toetsingsteam bestond uit vertegenwoordigers van het Havenbedrijf Rotterdam, Douane Rotterdam en de Zeehavenpolitie Rotterdam Rijnmond. Het team is in september 2003 gestart met zijn werkzaamheden en is na afloop in augustus 2004 weer ontbonden. Op incidentele, individuele basis zal indien nodig, een gelegenheidsteam worden gevormd om een nieuwe toetsing of hertoetsing uit te voeren.

Met de oprichting van het Toetsingsteam was de Rotterdamse organisatie voor havenbeveiliging compleet. Daarmee werd de fase van beleidsontwikkeling afgerond en kon het invoeringstraject beginnen.

6.2 Juridische kaders

Het juridische kader voor beoordeling van de veiligheid van de port facility in Europees verband is te vinden in diverse onderdelen van de EU Verordening. De basis is met name te vinden in artikel 15 van bijlage II waarin is bepaald dat de veiligheidsbeoordeling van de port facility wordt uitgevoerd door of namens de verdragsluitende staat op wiens grondgebied de port facility zich bevindt. Tevens zijn ook eisen gesteld aan degenen die de veiligheidsbeoordeling uitvoeren. Zo moeten deze personen over voldoende vaardigheden beschikken om de veiligheid van de port facility te kunnen beoordelen.

De beslissing van de burgemeester omtrent het al dan niet verlenen van instemming met het ingediende beveiligingsplan is op grond van de Algemene wet bestuursrecht (Awb) vatbaar voor bezwaar en eventueel beroep. Dit biedt dus de beheerder van de port facility de mogelijkheid in bestuursrechtelijke zin te ageren tegen een genomen besluit over het al dan niet goedkeuren van een beveiligingsplan. Bezwaar kan worden gemaakt binnen een termijn van zes weken na het genomen besluit namens de burgemeester. Als met de aanvraag wordt ingestemd en dus een certificaat wordt afgegeven zal normaliter geen bezwaar worden gemaakt. Bezwaren zullen met name worden ingediend als niet met de aanvraag wordt ingestemd. Ook kan een afgegeven certificaat worden ingetrokken.

Ook tegen het intrekken van een certificaat kan bezwaar worden gemaakt. De intrekingsgronden voor een reeds afgegeven certificaat zijn te vinden in artikel 9 van de Havenbeveiligingswet: als blijkt dat de beheerder van de port facility bij de aanvraag onjuiste of onvolledige gegevens heeft verstrekt waardoor bij aanvraag eigenlijk een negatief besluit zou moeten zijn genomen, indien blijkt dat de beheerder van de port facility heeft gehandeld in strijd met het beveiligingsplan of indien de beheerder heeft nagelaten te handelen in overeenstemming met het beveiligingsplan.

De burgemeester dient een afweging te maken van de rechtstreeks bij het te nemen besluit betrokken belangen (evenredigheidsbeginsel). De voor de belanghebbende (in dit geval beheerder van de port facility) nadelige gevolgen van het te nemen besluit mogen niet onevenredig zijn in verhouding tot de met het besluit te dienen doelen. Dit geeft de burgemeester dus de ruimte om de ernst van de overtreding door of het nalatig zijn van de beheerder van de port facility af te wegen tegen het gevolg van de afwijzing of intrekking (het niet meer mogen ontvangen van schepen).

In het verlengde van de bestuursrechtelijke mogelijkheden ligt de aansprakelijkheid en de eventuele schadeclaim (civielrechtelijk). Als in eerste instantie niet is ingestemd met het beveiligingsplan en na een beroepsprocedure op grond van de Awb blijkt dat bij de afweging op basis van het door het Toetsingsteam uitgebrachte advies is geconcludeerd dat dit ten onrechte is gebeurd of het evenredigheidsbeginsel is geschonden kan de overheid hiervoor aansprakelijk worden gesteld. De daaruit voortvloeiende geleden schade door het bedrijf zal in dat geval aanzienlijk zijn, aangezien zelfs schepen hebben moeten uitwijken, waarbij mogelijk flinke financiële belangen in het geding zijn.

In civielrechtelijk perspectief komt in dit verband ook de aansprakelijkheid van de overheid en van de individuele leden van het Toetsingsteam om de hoek kijken. Niet helder is of bijvoorbeeld nalatigheid van ambtenaren een onrechtmatige daad kan zijn. Het ligt nog gecompliceerder omdat het Havenbedrijf een verzelfstandigde overheids N.V. is. De genomen beslissingen zijn echter een gezamenlijk gedragen advies aan de burgemeester.

Indien een beheerder van een port facility bij de aanvraag onjuiste of onvolledige gegevens heeft verstrekt kan dit een grond vormen voor de burgemeester om de reeds gegeven instemming en het bijbehorende havenbeveiligingscertificaat in te trekken. Hoewel het verstrekken van onjuiste gegevens op zich ook strafbaar is vanuit strafrechtelijk perspectief lijkt deze weg niet opportuun. Immers door de mogelijkheid tot het intrekken van het certificaat kan de port facility al worden aangepakt. Ook bij het optreden en handelen van het Toetsingsteam op zich kan het strafrechtelijk perspectief in principe buiten beschouwing worden gelaten.

6.3 De werkwijze

Het Toetsingsteam staat onder leiding van het hoofd van de Zeehavenpolitie. Voor de dagelijkse coördinatie is een beroep gedaan op de Zeehavenpolitie (periode sept. 2003 – maart 2004) en het Havenbedrijf (april 2004 – sept. 2004). De coördinator neemt ook plaats in het ‘landelijk overleg Toetsingsteams’ dat gericht is op een landelijke uniformiteit te waarborgen in de uitvoering van de toetsingswerkzaamheden. In totaal zijn er zes leden van het Toetsingsteam, twee per kerndienst. Voor de nodige administratieve ondersteuning zijn twee medewerkers van respectievelijk de Douane en de Zeehavenpolitie aangetrokken.

Omdat verwacht werd dat het Toetsingsteam tegen strategische vraagstukken zou aanlopen waarover zij niet bevoegd is een beslissing te nemen, is tegelijkertijd de “stuurgroep Toetsingsteam” opgericht. De stuurgroep Toetsingsteam wordt gevormd door de directeur Havenbedrijf (voorzitter), het hoofd Zeehavenpolitie, het hoofd Douane Rotterdam, de coördinator Toetsingsteam, de Havenbeveiligingsofficier (Port Security Officer), het hoofd van de sector Port Security en de programmamanager Port Security van het Havenbedrijf. In het opgestelde draaiboek Toetsingsteam wordt de rol van de stuurgroep als volgt omschreven: “De stuurgroep neemt zelfstandig of op verzoek van het Toetsingsteam beslissingen inzake normering en interpretatie van de EU verordening / ISPS Code en de werkwijze van het Toetsingsteam”.

Het Toetsingsteam is in september 2003 van start gegaan. Op dat moment waren er nog maar tien maanden te gaan voordat de ISPS code van kracht zou worden. De eerste activiteit van het Toetsingsteam was het opstellen van een draaiboek waarin de werkwijze en de planning van het Toetsingsteam staat vastgelegd.

Het Toetsingsteam moest gedurende een relatief korte periode haar werkzaamheden verrichten. Om dit in goede banen te leiden is een harde planning opgesteld, gebaseerd op de wettelijke verplichtingen voor port facilities zoals die in de EU verordening staan beschreven. Voor 1 maart 2004 moet van iedere port facility in het competentiegebied een risicoanalyse zijn opgesteld. Uiterlijk op 1 juli 2004 moet iedere port facility beschikken over een goedgekeurd beveiligingsplan. Het Toetsingsteam heeft, met instemming van de stuurgroep, aan de port facilities de garantie afgegeven dat alle beveiligingsplannen die voor 1 mei 2004 werden ingediend tijdig (voor 1 juli 2004) zouden worden beoordeeld.

Het was een lastige taak om voor een complexe omgeving als het Rotterdams havengebied vast te stellen welke bedrijven over een port facility beschikken die vallen onder de ISPS code. Het havengebied is zo groot dat er jaarlijks vele bedrijven bijkomen en weggaan. Het Havenbedrijf Rotterdam beschikt niet over een kant-en-klaar systeem dat aangeeft welke bedrijven één of meer zeeschepen per jaar ontvangen. Die informatie moest daarom uit meerdere systemen worden geëxtraheerd. De zo ontstane lijst geeft een complete opsomming van alle locaties waar zeeschepen afmeren, locaties dus die per definitie ISPS plichtig zijn. Toch bleken er in deze lijst onvolkomenheden voor te komen. Vanwege het grote belang om over een complete en correcte lijst te beschikken is er een uitgebreide cross check uitgevoerd aan de hand van gegevens uit een ander bronstelsel (van de grafische afdeling van het Havenbedrijf), de adresgegevens uit het handelsregister van de kamer van Koophandel en de expertise van accountmanagers van de commerciële afdeling van het Havenbedrijf.

Direct bij de start van het Toetsingsteam is begonnen met de aanleg van dossiers op het niveau van de individuele port facility. Het betreffen hier zowel digitale dossiers als fysieke dossiers.

De eerste stap voor de port facilities in het traject van de ISPS code was het uitvoeren van een risicoanalyse. Op verzoek van het Toetsingsteam heeft de stuurgroep besloten dat aan de wettelijke eisen van een risicoanalyse is voldaan als 95% of meer van de vragen van de vragenlijst (de toolkit) is beantwoord. Uiteraard wordt wel van de port facilities verwacht dat men de vragenlijst naar waarheid invult. Dit wil dus zeggen dat men een situatie schetst van de stand van zaken zoals die zich op dat

moment voordoet. Om dit te waarborgen is een checklist opgesteld aan de hand waarvan de betreffende leden van het Toetsingsteam nagingen of de port facility een volledige en juiste weergave van de feiten heeft gegeven. Kennis van de haven en de hierin gevestigde bedrijven was bij dit onderdeel van groot belang voor een goede uitvoering van het werk. Hoewel de uiterste deadline voor het voltooien van de risicoanalyses op 1 maart 2004 lag heeft het Toetsingsteam er bij het bedrijfsleven op aangedrongen om voor 15 november 2004 middels de vragenlijst van de toolkit inzage te geven in de beveiligingssituatie van de port facility. Uit de gegevens die vervolgens ter beschikking zijn gesteld is gebleken dat bij ongeveer 50% van de ISPS plichtige bedrijven de risicoanalyse niet kon worden voltooid omdat men onvoldoende of geen gegevens ter beschikking stelde over de beveiligingssituatie van de port facility. Conform het draaiboek heeft het Toetsingsteam de zogenaamde achterblijvers benaderd. Middels een communicatietraject van telefoon, e-mail en persoonlijke gesprekken zijn de achterblijvers benaderd. Dit had een aanzienlijke verbetering van de respons tot gevolg. Bedrijven die desondanks toch niet meewerkten zijn vervolgens per brief door de Havenbeveiligingsofficier gewezen op de wettelijke verplichtingen en de mogelijke gevolgen voor het bedrijf als men hier niet aan voldoet.

In deze fase is ook de keuze gemaakt om per port facility een koppel van twee leden van het Toetsingsteam aan te wijzen. De vaste koppels zijn zodanig gekozen dat in geen van de drie koppels dezelfde dienst tweemaal vertegenwoordigd is. Tevens is de keuze gemaakt dat medewerkers van het Havenbedrijf, de enige kerndienst die zelf ook over port facilities beschikt, niet betrokken mogen zijn bij de toetsing van faciliteiten van het Havenbedrijf, zoals openbare kades, steigers en boeienspannen.

Tijdens het traject van risicoanalyse werd al snel duidelijk dat de te nemen maatregelen voor meerdere uitleg vatbaar waren. De port facilities vroegen om een duidelijke definiëring en een afbakening van de te nemen maatregelen. Al snel vroegen de port facilities ook om adviezen aan het Toetsingsteam over de te nemen beveiligingsmaatregelen. Binnen het Toetsingsteam en de Stuurgroep Toetsingsteam werd verschillend gedacht over het geven van advies. Het geven van een goed advies vergt een gedegen voorstudie van de beveiligingssituatie en kost dus tijd. Als eenmaal een aantal bedrijven is geadviseerd zou het een vorm van ongelijke behandeling zijn als dit bij andere bedrijven, in verband met tijdgebrek, zou moeten worden geweigerd. Deze ongelijke behandeling zou een goed argument geven bij eventuele bezwaar- en beroepprocedures als gevolg van non-compliance. Een ander risico van een adviserende rol is het mogelijke bezwaar hiertegen van commerciële beveiligingsbedrijven die advies tegen betaling geven. Deze branche zou een uitgebreide adviesrol van het Toetsingsteam als oneerlijke concurrentie kunnen beschouwen. Wellicht het zwaarst wegende bezwaar tegen het geven van advies is de dubbelrol die het Toetsingsteam daarmee op zich neemt. Bij het geven van advies zou het Toetsingsteam in de positie komen dat het maatregelen moet beoordelen die men zelf heeft aangedragen. De stuurgroep heeft dan ook snel besloten dat het geven van adviezen niet hoorde bij de taken van het Toetsingsteam, dit in tegenstelling tot de taakopvatting van het Toetsingsteam dat vooral de mogelijkheid zag om achterblijvers te helpen en zo te komen tot een snelle certificering van de port facility.

Ondanks deze substantiële risico's heeft het Toetsingsteam toch een beperkte adviserende rol gehad. In de praktijk blijkt het namelijk zo goed als onmogelijk om bedrijven niet te adviseren over de aanpak van de verplichtingen die door de ISPS code worden opgelegd. Regelmatig werd het Toetsingsteam geconfronteerd met vragen van bedrijven die bijvoorbeeld gingen over de hoogte van een hekwerk, de installatie van camera-systemen of het plaatsen van een slagboom. Aan het bedrijfsleven is duidelijk gemaakt dat aan deze adviezen geen rechten kunnen worden ontleend. Het geven van adviezen over een individueel beveiligingsvraagstuk is duidelijk als grens gesteld. Bedrijven die advies vroegen over een compleet beveiligingsconcept zijn altijd verwezen naar de beveiligingsexpertise die te koop is op de markt.

Het begrip prétoetsing is ingevoerd naar aanleiding van de discussie die is ontstaan over de adviesrol van het Toetsingsteam. In een poging om de adviesrol te beperken is aan de port facilities de mogelijkheid geboden om éénmalig een beveiligingsplan ter prétoetsing aan het Toetsingsteam aan te bieden. Hierbij golden twee belangrijke voorwaarden. Als eerste is gesteld dat alleen port facilities met

een hoog risicoprofiel in aanmerking kwamen. Ten tweede is gesteld dat een prétoetsing alleen wordt uitgevoerd als de te nemen maatregelen samenhangen met aanzienlijke investeringen. Naar mening van het Toetsingsteam en de Stuurgroep Toetsingsteam is op deze wijze tegemoet gekomen aan de behoefte voor advies maar zijn de risico's voor het Toetsingsteam tot een minimum beperkt.

Het voldoen aan de wettelijke verplichting voor de overheid om port facility beveiligingsplannen te beoordelen kan worden beschouwd als de meest belangrijke taak van het Toetsingsteam. De beoordeling van een beveiligingsplan is als volgt opgebouwd:

- Beoordeling van de volledigheid;
- Beoordeling van de kwaliteit;
- Beoordeling van de fysieke en procedurele invoering.

De volledigheid werd beoordeeld aan de hand van een uitgebreide checklist. Deze checklist is onderdeel van het draaiboek en is goedgekeurd door de stuurgroep Toetsingsteam. In de checklist komen alle verplichtingen, en aanbevelingen uit de ISPS code aan bod. Omdat vrijwel alle bedrijven gebruik maken van de toolkit is de indeling van de checklist hierop afgestemd.

Het beoordelen van kwaliteit is subjectief en valt niet met een uniforme checklist op te vangen. Bij dit onderdeel werd een beroep gedaan op de expertise en het gezond verstand van de leden van het Toetsingsteam. De leden van het Toetsingsteam moesten beoordelen of een bepaalde maatregel, fysiek of procedureel, in het plan voldoende is gewaarborgd en of deze maatregel zich verhoudt tot het risicoprofiel van de betreffende port facility. Vooral de procedures, die men verplicht is op te stellen, werden hierbij onder de loep genomen. Omdat het hier om een subjectief oordeel gaat, weliswaar van experts, is het van belang om bij twijfel een breed gedragen beslissing te nemen. De organisatie van het Toetsingsteam is dusdanig van opzet geweest dat de mogelijkheid om twijfelgevallen te bespreken ruim voor handen was. In eerste instantie leenden de dagelijkse briefing zich uitstekend om twijfelgevallen aan collega leden van het Toetsingsteam voor te leggen. Bij vraagstukken van strategische betekenis of bij aanhoudende twijfel werd een beroep gedaan op de stuurgroep. In een enkel geval zijn vraagstukken zelfs op landelijk niveau afgestemd alvorens een uitspraak volgde. Een goed voorbeeld hiervan is de onduidelijkheid die ontstond over de koppeling van de ISPS code en de Wet particuliere beveiligingsorganisaties en recherchebureaus (Wpbr). Pas nadat op ministerieel niveau hierover een beslissing was genomen kon het Toetsingsteam op dit gebied een definitief oordeel vellen.

Het laatste onderdeel van het beoordelen van het havenfaciliteit beveiligingsplan is het beoordelen van de fysiek genomen maatregelen. Met de politieterm "schouw" wordt in dit verband een beoordeling van de fysieke en procedurele invoering van een beveiligingsplan bedoeld. Een voorwaarde voor het verrichten van een schouw is dat het ingediende plan positief is beoordeeld in de eerste twee stappen.

In de meeste gevallen werd voor een schouw een hele of halve dag uitgetrokken. Bij enkele grote bedrijven met een hoog risicoprofiel kon dit oplopen tot wel twee dagen. Iedere schouw bestond uit drie onderdelen. Als eerste werd aan de hand van de ingevulde checklist het gehele plan stap voor stap doorgenomen. Eventuele onvolkomenheden en onduidelijkheden werden besproken. Na afloop van dit gesprek werd, wederom aan de hand van de checklist, doorgenomen welke onderdelen de leden van het Toetsingsteam graag zouden schouwen. Standaard hierbij was een ronde langs de buitengrens van de port facility, een gesprek met beveiligingspersoneel en het schouwen van de toegangspoort en het daar uitgevoerde toegangprotocol. Tenslotte presenteerden de leden van het Toetsingsteam in een afsluitend gesprek hun bevindingen aan de havenfaciliteit beveiligingsofficier. Eventuele onvolkomenheden op fysiek en procedureel niveau werden besproken waarbij de leden van het Toetsingsteam altijd probeerden direct tot afspraken over aanpassing of verbetering te komen. Het Toetsingsteam maakte bij iedere schouw aantekeningen die later werden verwerkt tot een schouwingverslag dat altijd op zo kort mogelijke termijn aan de havenfaciliteit beveiligingsofficier (port facility security officer) ter beschikking werd gesteld. In dit verslag werd een samenvatting gegeven van bevindingen van de leden van het Toetsingsteam. Tevens werden hierin de afspraken opgesomd die het Toetsingsteam met de beveiligingsofficier had gemaakt.



In de praktijk bleek al snel dat vrijwel geen enkele port facility bij de eerste schouw volledig positief kon worden beoordeeld. Dit was vooraf anders ingeschat en de beschikbare capaciteit van het Toetsingsteam was niet zodanig dat men ieder bedrijf meerdere malen kon bezoeken binnen de beperkte tijd die hiervoor beschikbaar was. Hier dient opgemerkt te worden dat het de eigen verantwoordelijkheid van de port facilities was om voor 1 juli 2004 aan de wetgeving te voldoen. De oplossing van het probleem is hier gevonden in proportionaliteit, in dit geval de proportionaliteit van de onvolkomenheden. Per port facility is beoordeeld met welke onvolkomenheden men toch in aanmerking kan komen voor certificering. Een eis is hierbij altijd geweest dat het beveiligingsplan zelf geen onvolkomenheden meer bevat. Een plan valt immers in een tijdsbestek van enkele weken gemakkelijk aan te passen maar de meeste fysieke of procedurele aanpassingen vergen meer tijd. Een tweede eis was dat het Toetsingsteam het vertrouwen moest hebben dat de openstaande opmerkingen binnen de daarvoor gestelde termijn zouden worden aangepakt. Dit beleid heeft er toe geleid dat de meeste bedrijven een herziene versie van hun beveiligingsplan hebben ingediend.

Conform het draaiboek Toetsingsteam werd op basis van een goedgekeurd havenfaciliteit beveiligingsplan een positief advies verstuurd aan de Havenbeveiligingsofficier (Port Security Officer) inzake het verstrekken van een Havenbeveiligingscertificaat namens de burgemeester. De betreffende port facility kreeg een afschrift van het door het Toetsingsteam geschreven advies. In dit advies zijn de openstaande bemerkingen van het Toetsingsteam nadrukkelijk meegenomen. In de meeste gevallen wordt in het advies een termijn genoemd waarbinnen de port facility geacht wordt de invoering van de fysieke en procedurele maatregelen te voltooien. Dit advies vormde in de periode na juli 2004 de basis voor de handhaving van de ISPS code.

De Havenbeveiligingsofficier heeft enkele dagen voor 1 juli 2004 een lijst gestuurd aan de Minister van Verkeer en Waterstaat waarin hij een opsomming geeft van de port facilities die door, lees namens, de burgemeester positief zijn beoordeeld en daarmee voldoen aan de ISPS code. Onder verantwoordelijkheid van de Minister zijn deze bedrijven vervolgens aangemeld bij de International Maritime Organisation (IMO). De IMO publiceert per 1 juli 2004 op Internet een overzicht waarin per

land en per haven wordt aangegeven welke bedrijven voldoen aan de ISPS code. Zo is na een lang en complex traject de juiste informatie aangekomen bij de bron waar de ISPS code is ontworpen.

7. Handhaven in Rotterdam

7.1 Handhaving in Rotterdam

De invoering van de ISPS code in de Rotterdamse haven kan succesvol worden genoemd. De top-down aanpak heeft niet geleid tot veel verzet bij de bedrijven in de haven. Uiteraard speelden economische motieven en het gevoel dat de maatregelen alleen maar bedoeld waren om de VS te beschermen een rol. Toch was het merendeel van de port facilities in de Rotterdamse haven op tijd gecertificeerd. Een aantal van de gecertificeerde port facilities heeft een tijdelijk certificaat gekregen omdat een aantal maatregelen, zoals het plaatsen van hekwerken, nog moest worden afgerond. Door het nemen van tijdelijke maatregelen voldeden zij echter wel aan de eisen van de ISPS volgens het advies van het Toetsingsteam. Voordat deze port facilities het certificaat voor vijf jaar krijgen zal er een hertoetsing plaatsvinden door het Toetsingsteam. Het is dus noodzakelijk om een goede beheersorganisatie te hebben die zorg draagt voor de administratie en het bijeenroepen van een Toetsingsteam als dat nodig is. Omdat het nemen van veiligheidsmaatregelen een jaarlijks terugkerende kostenpost is, is het voor de port facilities aantrekkelijk om als er geen aanslagen of andere criminele activiteiten plaatsvinden, de maatregelen te versoepelen of zelfs helemaal niet meer toe te passen. Als dat het geval is dan ontstaan de gevaren. Tijdens een uitzending van SBS6 in het voorjaar van 2004, nota bene tijdens de invoering van de ISPS code in Rotterdam, werd aangetoond dat het heel erg makkelijk is om op een haventerrein te komen en vervolgens naar de tankput te gaan om vervolgens "iets" te doen met de leidingen en tanks. Het is noodzakelijk dat de port facilities de security maatregelen handhaven en vooral naleven. Om dit te controleren en te handhaven is een organisatie nodig die de port facilities bezoekt en de maatregelen toetst.

De looptijd van het uitgereikte ISPS certificaat is maximaal vijf jaar. Voor het verstrijken van de looptijd dient een nieuwe toetsing plaats te vinden én advies te worden uitgebracht aan de Port Security Officer door het Toetsingsteam. Ook bij wijzigingen in de beveiligingsorganisatie of de infrastructuur van het bedrijf dient een hertoetsing plaats te vinden. De huidige handhavingstaak is door de burgemeester van Rotterdam neergelegd bij de havenautoriteit van Rotterdam, het Havenbedrijf Rotterdam. De Havenmeester is binnen het Havenbedrijf aangewezen als Port Security Officer. In zijn organisatie bestaat een "sector", bureau, Port Security dat belast is met onder andere de beheerstaken betreffende de ISPS code. Hiervoor is een administratie opgezet en worden aanvragen voor (her)toetsing verwerkt. Indien nodig, roept dit bureau de Toetsingsteamleden bijeen voor een beoordeling en toetsing van de security plannen en maatregelen. Een tweede functie van dit bureau is het aansturen van de controleurs Gevaarlijke stoffen van het Havenbedrijf Rotterdam om de werking van de security maatregelen te toetsen. Deze controleurs voeren de taken ten aanzien van de ISPS code uit naast hun dagelijkse werkzaamheden, controle op het vervoer en opslag van gevaarlijke stoffen in de Rotterdamse haven. Op basis van steekproeven en op basis van meldingen over de veiligheidsmaatregelen, door de overige handhavingsdiensten in de haven worden per maand een dertig tal port facilities bezocht. Na het bezoek aan de port facility worden de aangetroffen beveiligingsmaatregelen gerapporteerd aan het bureau Port Security. Indien nodig wordt door dit bureau actie ondernomen. Eén van de acties bestaat uit het contact opnemen met het bezochte bedrijf om uitleg te vragen over de waargenomen beveiligingsmaatregelen. Is het antwoord niet voldoende of bestaan er onduidelijkheden over de maatregelen dan kan het Toetsingsteam worden oproepen om nader uitleg te geven over de situatie of als het echt nodig lijkt, een hertoetsing uit te laten voeren. Komen de controleurs, de leden van het Toetsingsteam en de port facility niet tot overeenstemming over de te nemen acties dan kan het uiteindelijk zover komen dat er een negatief advies over de port facility wordt uitgebracht door het Toetsingsteam. Hiertegen is dan weer een bezwaar- en beroepsprocedure mogelijk. Het negatieve advies kan leiden tot het intrekken van het ISPS certificaat.

De Douane en de Zeehavenpolitie hebben ondanks hun bestaande bevoegdheden en betrokkenheid bij de invoering en toetsing van de ISPS code geen wettelijke handhavingstaak gekregen. Zij hebben enkel een signaleringsfunctie. Misstanden of gebreken dienen zij te rapporteren aan het Havenbedrijf Rotterdam. Het toezicht op en handhaving van de ISPS code bij de port facilities, is op grond van de

Havenbeveiligingswet vanuit het ministerie van Verkeer en Waterstaat geattribueerd naar de havengemeenten in Nederland. Als vorm van toezicht is gekozen voor rechtstreeks toezicht op de naleving door de havengemeenten zelf, het zogenaamde eerstelijnstoezicht. Systeemtoezicht, het zogenaamde tweedelijnstoezicht, ligt bij de Inspectie van Verkeer en Waterstaat (IVW). Naast de direct betrokken diensten in de haven is het de gemeente Rotterdam die verantwoordelijk is voor het eerstelijns toezicht op de naleving van de ISPS code. In de praktijk blijkt deze directe betrokkenheid minimaal. Alle verantwoordelijkheid is neergelegd bij de Havenmeester van Rotterdam als Port Security Officer. In de Leidraad Beveiliging Havens en Port Facilities [2003] is de volgende motivatie gegeven om de burgemeester aan te wijzen als havenautoriteit: er moet sprake zijn van een officiële bestuurlijke en juridische rechtspersoon of instantie; er mag geen sprake zijn van een politieke constellatie (College van B&W); de rechtspersoon of instantie dient in een hiërarchieke relatie te staan tot politie, havenautoriteiten en hulpdiensten en zijn rol dient inpasbaar te zijn in de calamiteiten- en rampenbestrijding; bij de keuze dienen handhaving en sanctiemogelijkheden een punt van overweging te zijn; bezwaar en beroep dienen mogelijk te zijn. Opmerkelijk is het om vast te moeten stellen dat de bevoegdheid om de Havenbeveiligingswet te handhaven bij het Havenbedrijf Rotterdam ligt. Het Havenbedrijf kent geen enkele hiërarchische relatie tot de Politie, Douane en overige hulpdiensten. Verder is sinds 1 januari 2004 het Havenbedrijf Rotterdam verzelfstandigd, waardoor commerciële belangen een rol zijn gaan spelen.

Het volgen van beleidsmatige zaken, agendering, besluitvorming en evaluatie, in zowel Nationaal als Europees verband en het participeren in diverse relevante werkgroepen ligt bij een andere directie van het Havenbedrijf Rotterdam. Op deze wijze wordt getracht een onafhankelijke positie van het bureau Port Security binnen het Havenbedrijf Rotterdam te garanderen.

De gemeente Rotterdam laat zich vertegenwoordigen in het Regionaal Beleidsoverleg Rampenbestrijding waarin ook het Havenbedrijf Rotterdam, de Politie en de Douane zijn vertegenwoordigd. In diverse werkgroepen is een lid van de Algemene Bestuursdienst Rotterdam aanwezig waardoor de burgemeester op de hoogte is van de relevante zaken. Het ontbreekt echter aan directe sturing of grip op de situatie. Veel vertrouwen is er op de samenwerking tussen de betrokken overheidsdiensten. Samenwerking waar het volgens mij nogal eens aan ontbreekt. Zo zijn de Politie, Douane en Koninklijke Marechaussee gezamenlijk bezig een visie te ontwikkelen op de security in de haven en de daarbij behorende taken en bevoegdheden van deze diensten. Zij doen dit zonder het Havenbedrijf en de gemeente Rotterdam. Juist een integrale visie is van groot belang in de strijd tegen het terrorisme.

7.2 De drie fasen

De invoering van de ISPS code is pas de eerste stap in de keten van security. In totaal worden drie fasen onderscheiden. De eerste fase van de drie fasen werd in principe afgerond op 1 juli 2004 met de invoering van de ISPS code en de afgeleide EU Verordening. Toetsing en certificering hebben vervolgens plaatsgevonden. De nationale wetgeving is hierbij verankerd in de Havenbeveiligingswet die van kracht is geworden per augustus 2004. De verantwoordelijkheid voor het invoeringproces ligt bij de Minister van Verkeer en Waterstaat, als nationale bevoegde autoriteit en de burgemeesters van zeehavens als de lokale bevoegde autoriteit. De uitvoering van de beheerstaken en de handhaving van de regelgeving is neergelegd bij de betrokken havendiensten. Toetsing van de plannen en beveiligingsmaatregelen is een gezamenlijke actie geweest van het Havenbedrijf Rotterdam, de Politie en de Douane. De toetsing en het certificeringstraject zal een continu proces zijn als gevolg van de dynamiek van een haven in ontwikkeling. Bedrijfsstructuren zullen blijven veranderen en nieuwe spelers zullen zich aandienen.

De tweede fase betreft de havengebieden als geheel, port facilities, overige bedrijven en (natte en droge) infrastructuur. In deze tweede fase zal vanuit de Europese Unie worden voorgeschreven dat havengebieden met ISPS plichtige port facilities tevens dienen te beschikken over een overall Port Security Plan (Havenbeveiligingsplan). Een voorstel voor een richtlijn van het Europees Parlement en van de Europese Raad, betreffende het verhogen van de veiligheid van de havens als geheel, bevindt

zich inmiddels in de afrondende fase. De havenbeveiligingsplannen zullen niet alleen betrekking hebben op de ISPS plichtige bedrijven, maar ook op de overige bedrijven in het havengebied en de aanwezige infrastructuur. De definitieve kaders van de maatregelen worden medio 2005 verwacht en naar verwachting zal de uitvoering in de tweede helft van 2006 zijn beslag moeten krijgen. Vooruit lopende op deze maatregelen is in Rotterdam een aanvang gemaakt met het aanwijzen van vitale infrastructuur en het analyseren van de mogelijke risico's. Dit heeft plaatsgevonden in samenwerking tussen de gemeente Rotterdam, het Havenbedrijf Rotterdam, de Politie en de Douane. De leden van het Toetsingsteam ISPS zijn hierbij niet betrokken geweest. Mogelijk zullen de leden van het Toetsingsteam ISPS een rol gaan spelen in de toetsing van de security plannen en maatregelen. Een landelijk project, uitgevoerd door TNO, om de vitale infrastructuur in kaart te brengen heeft parallel maar afzonderlijk gelopen aan dit project in Rotterdam.

De derde fase omvat de zogenaamde keten security, waarbij het gehele logistieke proces van producent tot afnemer onderwerp zal zijn. Op basis van certificering van de betrokken sectoren en bedrijven, alsmede met de inzet van nieuwe en bestaande technologie is het de bedoeling te komen tot een totale beveiliging van de logistieke keten. Deze fase zal vermoedelijk niet direct dwingend worden opgelegd. Maar door de aanwezige economische belangen zal voor het bedrijfsleven deelname in de meeste gevallen een "must" zijn vanuit economisch oogpunt. Een invoering datum staat nog niet vast. Naar verwachting zal een aantal stappen versneld ter uitvoering worden gebracht gezien de Brusselse ontwikkeling op het gebied van met name de Authorised Economic Operator (AEO), maar ook de mondiale ontwikkelingen met betrekking tot supply chain security. Welke diensten betrokken zullen zijn en op welke wijze is nu nog niet duidelijk.

Interessant wordt het om het proces van invoering van de tweede fase te gaan volgen, top-down of bottom-up. Komt er aanvullende wetgeving en zo ja, welke minister wordt hiermee belast. Wie wordt de verantwoordelijke lokale autoriteit? Worden er afzonderlijke plannen gemaakt per bedrijf, infrastructurele kunstwerken? Gaan er weer overheidsdiensten deelnemen, wordt er gebruik gemaakt van het bestaande toetsingsteam?

7.3 Informatie

Naast toezicht en handhaving is het delen van informatie een belangrijk punt. Nu is het uitwisselen van informatie wettelijk niet mogelijk. Vanuit de optiek van security is het juist essentieel dat de aanwezige "awareness" wordt verbreed. Dit geldt zowel voor de betrokken bedrijven en de overheidsdiensten in de haven. Het tijdig beschikken over juiste en volledige informatie blijft het machtigste wapen tegen terrorisme en criminaliteit. Vanuit een optimale informatiehuishouding, informatiepositie en een juiste analyses is een overheidsdienst in staat adequaat te handelen. In de huidige situatie is de informatiepositie van de betrokken overheidsdiensten niet optimaal te noemen. Informatie met betrekking tot security incidenten blijft nu zweven bij de afzonderlijke diensten. Zowel in- als extern blijft informatie hangen of is het niet mogelijk deze te delen. Buiten wettelijke beperkingen spelen ook organisatorische en technische problemen. Momenteel is het alleen mogelijk informatie te delen na toestemming van het Openbaar Ministerie. Er is een proces op gang gebracht om de onderkende gebreken in de wetgeving aan te passen. Technisch is het mogelijk systemen aan elkaar te koppelen, echter dit vergt grote investeringen en levert problemen op ten aanzien van afscherming en beveiliging.

In de zogenaamde september brief van 10 september 2004 aan de Tweede Kamer doet de Nationaal Coördinator Terrorismebestrijding [2004] voorstellen voor maatregelen om terrorisme te bestrijden in Nederland. Ten aanzien van het delen van informatie stelt de Nationaal Coördinator Terrorismebestrijding dat een van de punten voor een doeltreffende aanpak van terrorismebestrijding is het combineren, veredelen en gebruiken van informatie zoals deze door derden wordt verzameld. Het concentreren van de personen die belast zijn met de informatieverzameling bij de Algemene Inlichtingen en Veiligheidsdienst, Militaire Inlichtingen en Veiligheidsdienst (MIVD), Koninklijke Marechaussee (Kmar), politie en andere informatiediensten binnen één dienst is geen oplossing want dan wordt het contact verloren met de moederorganisaties. Voor de bevoegdheden die moeten worden

ingezet bij de bestrijding van terrorisme geldt in beginsel hetzelfde. Dit betekent dat in Rotterdam niet één bureau kan komen waar de betrokken overheidsdiensten zouden kunnen samenwerken aan het verzamelen en veredelen van informatie. Landelijk wordt een samenwerkingsverband gestart. De participanten hierin zijn: AIVD, MIVD, politie, OM en de Immigratie- en Naturalisatiedienst (IND). Deze diensten hebben hun informatie uitwisseling geïntensiveerd door de inrichting van den Contra-Terrorisme-infobox (CT-infobox). Dit is een informatieknooppunt en analyse eenheid. Verschillende informatiebestanden worden op deze wijze met elkaar gecombineerd, de informatie wordt vervolgens aan een multidisciplinaire beoordeling onderworpen om operationele acties te bepalen.

8. Invoering, een analyse

8.1 Overzicht

Hoe is de invoering van de ISPS code verlopen in de Rotterdamse haven? In de voorgaande hoofdstukken is een aantal stappen die genomen zijn uitvoerig besproken. Ik zal nu dieper ingaan op de wijze waarop vervolgens invoering heeft plaatsgevonden en wat dat heeft betekend voor de Rotterdamse haven. Als eerste een kort, chronologisch overzicht van de reeds eerder genoemde relevante gebeurtenissen.

Na de tragische gebeurtenissen van 11 september 2001 is op de vergadering van de IMO, november 2001, overeengekomen nieuwe maatregelen voor de beveiliging van schepen en port facilities te ontwikkelen. Hiertoe is een werkgroep vanuit de Commissie maritieme veiligheid ingesteld die voor december 2002 haar adviezen heeft uitgebracht.

In december 2002 heeft de Diplomatieke Conferentie van de IMO deze wijzigingen op het bestaande SOLAS-verdrag van 1974 aangenomen. Deze maatregelen zijn gericht op het geven van invulling aan beveiligingsmaatregelen in de maritieme sector. Deze aanvulling op het SOLAS-verdrag is de International Ship and Port Facility Security code en bestaat uit twee delen. Deel A bestaat uit verplichte maatregelen, deel B bestaat uit een groot aantal aanbevelingen.

In het Port Security Policy Board, te Rotterdam is begin 2003 besloten tot oprichting van een multidisciplinair Toetsingsteam bestaande uit leden van het Havenbedrijf Rotterdam, Douane Rotterdam en de Zeehavenpolitie Rotterdam Rijnmond. Op dat moment bestond de Port Security Development Group (PSDG) al. De PSDG was opgericht voor het geven van preventie adviezen op het gebied van criminaliteitsbeheersing en als zodanig bezig met het ontwikkelen van hulpmiddelen om het bedrijfsleven bij te staan in de strijd tegen de criminaliteit. Er werden door de PSDG workshops georganiseerd, een toolkit criminaliteitspreventie ontwikkeld en een gids, Security Mainport Rotterdam geschreven. Al snel werd de aandacht van de PSDG verlegd naar terrorisme. De bestaande ideeën over de toolkit werden aangepast richting ISPS waardoor snel ingespeeld kon worden op de vraag vanuit het bedrijfsleven om een handvat te ontwikkelen dat bruikbaar zou zijn voor de bedrijven in de Rotterdamse haven.

Door de werkgroep Security Zeehavens en Port Facilities, bestaande uit vertegenwoordigers van Groningen Seaports, Gemeentelijk Havenbedrijf Amsterdam, het toenmalige Gemeentelijk Havenbedrijf Rotterdam, gemeente Den Haag, Ondernemingsvereniging Regio Amsterdam, Deltalinqs Rotterdam, Port Security Development Group Rotterdam, FNV Bondgenoten, Inspectie Verkeer en Waterstaat en het Directoraat-Generaal Goederenvervoer, is half 2003 een leidraad opgesteld om het bedrijfsleven te ondersteunen om te voldoen aan de wettelijke eisen en hierbij in ogenschouw te nemen de mate van proportionaliteit.

Het Toetsingsteam is in september 2003 van start gegaan. Een van de eerste activiteiten was het opstellen van een draaiboek waarin de werkwijze en de planning van het Toetsingsteam is vastgelegd. Het Toetsingsteam moest in een relatief korte periode, september 2003 tot juli 2004, haar werkzaamheden verrichten. Omdat de mogelijkheid bestond dat het Toetsingsteam tegen strategische vraagstukken zou aanlopen waarover zij geen beslissingsbevoegdheid heeft, is een stuurgroep Toetsingsteam opgericht. Deze stuurgroep werd gevormd door de directeur Havenbedrijf Rotterdam, het hoofd Zeehavenpolitie, het hoofd Douane Rotterdam, de leider Toetsingsteam, de (beoogd) Port Security Officer (de Havenmeester van Rotterdam), het hoofd van de sector Port Security van het Havenbedrijf Rotterdam en de programmamanager Port Security van het Havenbedrijf Rotterdam.

In het voorjaar van 2004 zijn de, door de port facilities ingevulde risk assessments, beoordeeld door de leden van het Toetsingsteam. Kort daarna zijn de eerste beveiligingsplannen beoordeeld en heeft een fysieke schouw plaats gevonden van de port facility.

In EU-verband is de juridische basis voor de regelgeving vast gelegd in Verordening (EG) Nr. 725/2004 van 31 maart 2004 van het Europese Parlement en de Raad betreffende de beveiliging van schepen en port facilities (hierna EU Verordening). Met deze Verordening wordt de basis gelegd voor een geharmoniseerde invoering van eerdergenoemde ISPS code in EU-verband.

Hoewel de EU Verordening rechtstreeks in de Lidstaten werkend is, moest voor de invoering van de EU Verordening in Nederland een nieuwe nationale uitvoeringswet gemaakt worden; de Havenbeveiligingswet. Gezien de krappe tijd heeft de Minister van Verkeer en Waterstaat middels een brief bij de Eerste Kamer op 25 juni aangedrongen het wetsvoorstel met voorrang te behandelen. De Havenbeveiligingswet is op 5 juli 2004 vastgesteld en op 15 juli 2004 gepubliceerd in de Staatscourant. De argumenten die de Minister heeft gebruikt om de wet snel behandeld te krijgen waren onder andere de economische belangen die er mee gepaard gaan en het voorzitterschap van de EU door Nederland dat een voorbeeldfunctie met zich meebrengt.

Begin april 2004 werden de eerste certificaten aan port facilities in de Rotterdamse haven die voldeden aan de eisen van de ISPS code door de burgemeester van Rotterdam uitgereikt, in aanwezigheid van de Minister van Verkeer en Waterstaat.

Per 1 juli 2004 waren ongeveer 125 port facilities in de Rotterdamse haven gecertificeerd.

8.2 Top-down

De wijze waarop de invoering van de ISPS code heeft plaatsgevonden kan getypeerd worden als een top-down invoering. De wijze waarop het gehele proces werd bestuurd was een vorm van “enforcement”. Dit is niet zo verwonderlijk omdat de beschikbare tijd om nationale wetgeving te maken, als uitwerking van internationale wetgeving en vervolgens te invoeren, beperkt was.

Na de aanslagen van 11 september 2001 is op initiatief van de VS in internationaal verband gestart met het leggen van een fundament voor een nieuw beveiligingsregiem voor onder andere de maritieme sector (havens en zeescheepvaart). De VS waren vooral bezig met de beveiliging van hun eigen territorium. Zij probeerden daarbij de toegang tot de grens als het ware zover mogelijk bij de eigen landsgrenzen vandaan te leggen. Al het inkomende verkeer voor de VS moest gecontroleerd worden bij het verlaten van het land van vertrek. Dit soort “nationale” wetgeving wereldwijd geïmplementeerd krijgen is onmogelijk. De VS hebben dan ook gezocht naar een mogelijkheid om snel en efficiënt de eigen wetgeving internationaal geïmplementeerd te krijgen. De mogelijkheid werd gevonden in een uitbreiding van het bestaande SOLAS verdrag met de ISPS code. Begrijpelijk is het dat na de aanslagen in de VS en bedreigingen van terrorisme wereldwijd gezocht werd naar mogelijkheden om te voorkomen dat terroristische aanslagen plaats zouden vinden. Maar of de maatregelen die de VS beoogd hebben op te nemen in internationale wetgeving (gericht op de veiligheid van mensenlevens op zee) in overeenstemming zijn met de aard van het beoogde beleid, om terrorisme te voorkomen in de VS wordt door mij betwijfeld. Het lijkt er op dat de VS gebruik hebben gemaakt van de mogelijkheid snel wereldwijd wetgeving te invoeren vooral ter bescherming van hun eigen belangen.

8.3 Policy window

In een korte tijd is in Rotterdam veel gebeurd. In december 2002 is de IMO wetgeving tot stand gekomen, begin 2003 is besloten tot de oprichting van een Toetsingsteam en op 1 juli 2004 was de wetgeving geïmplementeerd. Was er in Nederland of in Rotterdam sprake van een Policy window?

Binnen het Havenbedrijf Rotterdam is er hard gewerkt om te zorgen dat Nederland op tijd klaar zou zijn met de invoering en het certificeren van de port facilities. Het Havenbedrijf Rotterdam geeft aan dat het investeren in port security, in dit geval beveiliging in algemene zin, een aantal voordelen oplevert [scriptie Risicomanagement, 2004]. Het eerste punt is een economisch punt. Bij een gezamenlijke aanpak kan de kennisopbouw effectief verlopen waarmee de kosten per bedrijf of port

facility laag kunnen worden gehouden. Een ander punt betreft het imago van Rotterdam. Het bestuur van Rotterdam was bezig met het verbeteren van het kwaliteitsimago van de stad, een onderdeel daarvan is het verbeteren van de veiligheid. Het derde genoemde punt betreft invloed. Interne kennisopbouw in een vroeg stadium biedt mogelijkheden om invloed uit te oefenen tijdens de totstandkoming van wetgeving die internationaal, nationaal en lokaal getroffen moesten worden. Op deze wijze kon vermeden worden dat regelingen zouden worden getroffen die nadelig zouden zijn voor Rotterdam. Duidelijk is dat het Havenbedrijf Rotterdam een belangrijke rol heeft gespeeld bij het proces van beleidsformulering, invoering en uitvoering. Het Havenbedrijf Rotterdam ziet de ISPS code als een eerste station bij het verhogen van de veiligheid in de Rotterdamse haven.

Het Havenbedrijf Rotterdam kent met name een hoge prioriteit toe aan economische factoren. De snelheid waarmee de verladingen kunnen plaatsvinden, bepalen de kosten van het verladen. Security maatregelen kosten geld en kunnen leiden tot vertraging van de processen. Om een aantrekkelijke haven te zijn, of te blijven, moet er snel gewerkt kunnen worden. Schepen moeten binnen kunnen komen, gelost worden en weer vertrekken zonder oponthoud. Door op een juiste wijze betrokken te zijn bij de totstandkoming van de wetgeving heeft het Havenbedrijf een grote invloed gehad op de nationale wetgeving. Doordat het Havenbedrijf ook aanwezig was bij de IMO vergadering kon goed worden ingespeeld op wat komen ging. Er is echter geen sprake van een Policy window, wel van beïnvloeding en anticiperen.

Het is overigens de vraag of het ministerie van Verkeer en Waterstaat gebruik heeft gemaakt van een Policy window. Gezien de tijd die het heeft gekost om nationale wetgeving te maken en door de Kamer te laten goedkeuren lijkt het er op dat het ministerie geen concept wetgeving had klaarliggen. Het lijkt of gewacht is op EU regelgeving zonder zelf gebruik te maken van de mogelijkheden. Ik heb verder geen onderzoek gedaan om een antwoord te krijgen op deze vraag omdat dit buiten de scope van mijn scriptie valt. Dat er nationale wetgeving zou komen was toch wel voorspelbaar.

8.4 Kritiek

Kritiek op de top-down benadering wordt door Hill onderscheiden in drie vormen: 1) kritiek op de aard van het beleid, 2) kritiek op het onderlinge verband tussen beleidsformulering en het invoeringproces en 3) kritiek op de normatieve uitgangspunten.

De kritiek van Hill op de top-down invoering is in dit geval duidelijk als het gaat over de aard van het beleid. De VS proberen met de ISPS code hun grondgebied te beschermen tegen terrorisme. Uiteindelijk wordt de beveiliging van het Amerikaanse contingent door internationale wetgeving over de rug van andere landen geïmplementeerd. In hoeverre zijn andere landen betrouwbaar als het gaat om de invoering van dit soort wetgeving? In hoeverre wordt internationale wetgeving in dat land gehandhaafd? In vele landen, waaronder de Derdewereldlanden, ontbreekt het aan financiële middelen of aan enige vorm van sense of urgency omdat het probleem van beveiliging tegen terrorisme vooral als een probleem van de Westerse wereld of specifiek van de VS wordt gezien. Grootschalige terroristische aanslagen komen, in de vaak arme landen niet voor omdat terroristische aanslagen tot doel hebben vooral de rijke, Westerse landen te treffen.

Tijdens de invoering van de ISPS in Rotterdam waren het vooral de economische belangen die een grote rol speelden bij de bedrijven die de security maatregelen moesten treffen. Zij ervoeren de maatregelen vooral als maatregelen om de VS te beschermen tegen terrorisme en helemaal niet als maatregelen om het schip en haar bemanning te beschermen. Bedrijven bleken enigszins welwillend te zijn als het gaat om het nemen van maatregelen als dat financiële voordeel ging opleveren voor de verzekering tegen criminaliteit. De financiële consequenties waren soms aanzienlijk terwijl er geen financiële tegemoetkoming tegenover stond. Dit in tegenstelling tot de VS waar de overheid financiële middelen vrij hadden gemaakt voor het nemen van maatregelen. Als de Rotterdamse bedrijven de maatregelen niet zouden nemen konden de financiële consequenties groter zijn dan de investeringen in maatregelen. Schepen en rederijen zouden geen gebruik meer maken van die port facility als het bewuste schip naar de VS zou varen. Op grond van de komst van een niet gecertificeerde port facility

zullen de VS een schip weigeren in een Amerikaanse haven. De Rotterdamse bedrijven hadden geen andere keus dan te investeren in maatregelen, veel zeescheepvaart komt of gaat naar een Amerikaanse haven. Het ministerie van Verkeer en Waterstaat heeft uiteindelijk een subsidie per port facility (500 euro) toegezegd aan het Havenbedrijf Rotterdam. Het Havenbedrijf Rotterdam heeft dit geld indirect ten goede laten komen aan de Rotterdamse bedrijven door het geld te gebruiken voor de ontwikkeling van de eerder besproken toolkit. Tijdens voorlichtingsbijeenkomsten, georganiseerd door het Havenbedrijf Rotterdam, en tijdens gesprekken tussen ondernemers en de leden van het Toetsingsteam kwamen deze bezwaren telkenmale naar voren.

Kritiek op het onderlinge verband tussen beleidsformulering en het invoeringproces komt naar voren als het gaat over het zogenaamde level playing field. Een veel gehoorde klacht van de bedrijven was dat het level playing field in Europa onder druk stond. In eerste instantie hadden een groot aantal bedrijven alleen het idee dat binnen Europa grote verschillen bestonden in de invoering van de ISPS code. Vooral de te nemen maatregelen en de controle daarop, waren volop onderwerp van discussie. Deze discussie werd in tweede instantie versterkt doordat bedrijven naast vestigingen in Rotterdam ook vestigingen hebben in onder andere België en Duitsland. Bezoeken aan havens in België, Duitsland en Engeland door collega's van het Toetsingsteam bevestigen het beeld dat op verschillende wijzen de invoering heeft plaatsgevonden. De uitvoeringsmaatregelen, de financiële tegemoetkomingen en de wijze van beoordelen en certificeren verschillen per land. Nederland, en in het bijzonder Rotterdam, wil graag aan de eisen van de ISPS voldoen en was er dan ook alles aan gelegen om voor 1 juli 2004 klaar te zijn; het beste jongetje van de klas willen zijn. Dit streven is mogelijk ook ingegeven doordat vanaf die datum Nederland voorzitter was van de EU. Het op tijd klaar zijn moest dienen als een voorbeeld voor de overige Lidstaten. De kritiek is vooral terug te voeren op de late totstandkoming van de nationale wetgeving in relatie tot het moment van starten van het invoeringproces. Door voorop te willen lopen ten aanzien van het invoeren binnen de EU zat er een gat tussen beleidsformulering en invoering in tijd gezien. Sterker nog, de twee fasen van de beleidscyclus werden omgedraaid. Het onderlinge verband op het gebied van inhoud van het te formuleren beleid en invoering werd beïnvloed door het Havenbedrijf Rotterdam, in de volgende paragraaf, "anticiperen op te ontwikkelen beleid", kom ik hierop terug.

Kritiek uit oogpunt van normatieve uitgangspunten is ook mogelijk. Uitgangspunt van de VS is dat het mogelijk is terroristische aanslagen te voorkomen door het invoeren van maatregelen in andere landen. Met het invoeren van maatregelen tegen terrorisme vanuit andere landen dan de VS, voorkom je niet dat terroristen of middelen voor terroristische activiteiten het land binnenkomen. In dit geval leiden vele wegen naar het uiteindelijke doel van een terrorist. Voorkomen van terrorisme is blijkbaar onmogelijk zolang er grote verschillen bestaan in welvaart en culturen. Het voeren van oorlog tegen Islamitische landen of landen die terroristen steunen is geen oplossing, een strijd tegen het moslim fundamentalisme lijkt uiteindelijk alleen maar meer strijd op te roepen.

Van de Graaf en Hoppe noemen nog een punt van kritiek wat ik bij het bespreken van de top-down benadering wil aanroeren. Door de nadruk te leggen op conformiteit tussen beleid-als-plan en beleidsuitvoering verduistert het top-down perspectief het onderscheid tussen intelligente aanpassing van beleid en een simpele afwijking van het gestelde beleid. Actoren in het betreffende beleidsveld zijn vaak vindingrijker dan de beleidsmakers. In de praktijk verliep dit anders. Ik zal een beeld schetsen. De rol van het Toetsingsteam tijdens de invoering is een heel belangrijke rol geweest. Het Toetsingsteam was enerzijds het klankbord voor de Stuurgroep om strategische vraagstukken te beantwoorden en voor het Havenbedrijf om ideeën te genereren ten aanzien van de wetgeving. Anderzijds was het vooral het Toetsingsteam dat adviezen gaf aan de port facilities omdat niet altijd duidelijk was wat er verwacht werd of wat de eisen vanuit de EU Verordening waren. Over deze laatste rol is veel gesproken. Hoe kan een Toetsingsteam een advies geven over beveiligingsvraagstukken en vervolgens een toetsende rol vervullen. Theoretisch zou het zo kunnen zijn dat het advies van een Toetsingsteam wordt afgekeurd door andere leden van het Toetsingsteam. Juist door deze positie, weten wat er speelt bij de te toetsen port facilities, weten welke strategische vraagstukken er liggen bij de Stuurgroep en het direct benaderbaar zijn van de Toetsingsteamleden door medewerkers van het Havenbedrijf en omgekeerd, konden de Toetsingsteamleden de

medewerkers van het Havenbedrijf benaderen die bezig waren met de wetgeving. Tevens kon geanticipeerd worden op de nieuwe wetgeving. Sterker nog, aan de hand van de praktijk werden voorstellen gedaan door het Havenbedrijf aan het ministerie van Verkeer en Waterstaat voor de nieuwe Havenbeveiligingswet.

8.5 Anticiperen

Direct vanaf het begin, toen sprake was van de komst van internationale wetgeving is in Rotterdam geanticipeerd op hetgeen komen zou. De burgemeester van Rotterdam werd daarbij geadviseerd door zijn adviseurs vanuit de Port Security Policy Board. Het belangrijkste punt was dat de verantwoordelijkheden en bevoegdheden van de betrokken partijen moesten worden vastgelegd. Daarnaast werd besloten tot oprichting van een multidisciplinair Toetsingsteam. Het Toetsingsteam is in september 2003 van start gegaan. Een van de eerste activiteiten was het opstellen van een draaiboek waarin de verantwoordelijkheden en werkwijze en planning van het Toetsingsteam zijn vastgelegd. Al snel waren de verantwoordelijkheden duidelijk, helder en geaccordeerd door de betrokken partijen in Rotterdam. De directie van het Havenbedrijf Rotterdam is een key player in het geheel. Toch is het de burgemeester van Rotterdam geweest die alle eindverantwoordelijkheid heeft behouden. Uitvoering van de maatregelen heeft hij neergelegd bij de beoogd Port Security Officer (de Havenmeester van Rotterdam), de leiding over het Toetsingsteam heeft hij vanuit het oogpunt van voorkomen van belangenverstrengeling neergelegd bij het Hoofd van de Zeehavenpolitie.

Anticiperen op te ontwikkelen beleid. De invoering van de ISPS code moest snel gebeuren omdat de internationale wetgeving in december 2002 tot stand gekomen was en de deadline van inwerkingtreden gesteld was op 1 juli 2004. Het Toetsingsteam, dat adviezen moest geven aan de burgemeester of een port facility wel of niet voldeed aan de ISPS code, werd pas in september 2003 opgericht door de Port Security Policy Board. Europese en nationale wetgeving waren toen nog niet klaar, deze bevonden zich beide nog in de beleidsbepalingfase. Toch zijn er in die periode door de leden van het Toetsingsteam beveiligingsplannen beoordeeld, port facilities geschouwd en adviezen uitgebracht aan de burgemeester van Rotterdam. Omdat de IMO al begin 2003 de ISPS code gereed had, waren de minimale eisen waaraan voldaan moest worden al bekend bij, met name, het Havenbedrijf Rotterdam. Zo kon worden geanticipeerd op de te nemen besluiten door de EU en het nationale parlement, initiatiefnemer hierbij was de werkgroep Security Zeehavens en Port Facilities.

Tot 1 juli 2004 was er sprake van een interim periode waarin de te nemen beveiligingsmaatregelen hun beslag dienden te krijgen. Voor de in deze periode te verrichten werkzaamheden is een zogenaamde "Voorlopige Leidraad Beveiliging Havens en Port Facilities" opgesteld door de werkgroep Security Zeehavens en Port Facilities. De Leidraad diende als uitgangspunt voor de werkzaamheden van het Toetsingsteam. Mede doordat het Toetsingsteam een multidisciplinair team was, bestaande uit medewerkers van het Havenbedrijf Rotterdam, Douane en Zeehavenpolitie, was veel kennis in huis. Deze kennis maakte het mogelijk op een adequate wijze de werkzaamheden te verrichten en zelfs input te leveren voor de nationale wetgeving. De nationale wetgeving, de Havenbeveiligingswet is dus conceptueel beïnvloed geweest door het Havenbedrijf Rotterdam. De (wets)tekst is weliswaar van het ministerie van Verkeer en Waterstaat maar de voorzet voor de wet komt uit de Expertgroep (bestaande uit: vertegenwoordigers van het ministerie van Verkeer en Waterstaat, havenbedrijven en politie) die op haar beurt flink werd voorbereid door de werkgroep Havens, waarvan het Havenbedrijf Rotterdam voorzitter is. Verder is het Havenbedrijf Rotterdam achter de schermen aan het lobbyen geweest om de ISPS code niet een kopie te laten zijn van de U.S. Coastguard regels. De Coastguard regels werden als niet uitvoerbaar beschouwd. De drang tot lobbyen is te verklaren omdat het Havenbedrijf Rotterdam zichzelf zag als vertegenwoordiger van de (toen nog) grootste haven ter wereld. Duidelijk wordt wel dat vervlechting hier heeft gewerkt, een verzelfstandigd overheidsorgaan dat gebruik weet te maken van de mogelijkheden. De formele macht ligt echter bij de Minister van Verkeer en Waterstaat.

Het Havenbedrijf Rotterdam is niet of nauwelijks betrokken geweest bij de totstandkoming van de ISPS code. Een van de medewerkers is in 2002 aanwezig geweest bij de vergadering over de invulling

van deze nieuwe internationale wetgeving. Door de aanwezigheid van deze medewerker was het echter wel mogelijk te anticiperen op de komende wetgeving. Hierdoor had het Havenbedrijf Rotterdam een informatie voorsprong ten opzichte van de overige diensten in de Rotterdamse haven. De overige diensten, leden van de Port Security Policy Board, zijn niet betrokken geweest bij de totstandkoming. Zij waren dus volledig afhankelijk van de informatie die aanwezig was bij het Havenbedrijf. Bij de totstandkoming van de EU Verordening is het Havenbedrijf Rotterdam, evenals de overige leden van de Port Security Policy Board, niet betrokken geweest. Dit was vooral een aanscherping van de regels die al in de ISPS code waren opgenomen. Ik heb geen informatie over eventuele pogingen van het Havenbedrijf om hieraan deel te nemen.

Het succes van de invoering van de ISPS code is vooral te danken aan de wijze waarop geanticipeerd is door het Havenbedrijf Rotterdam. Zonder deze betrokkenheid was het niet mogelijk geweest op tijd klaar te zijn met de invoering voor 1 juli 2004. Door het Havenbedrijf Rotterdam is een balans gevonden tussen enerzijds de private (commerciële) taken en anderzijds de publieke taak van Havenmeester. Toch is de verwevenheid van bevoegdheden en de belangen een punt van aandacht. In de paragraaf over Policy windows zal ik de motivatie van het Havenbedrijf bespreken.

Anticiperen op beleidstoepassing. Ver voordat de Havenbeveiligingswet was gepubliceerd waren de eerste bedrijven al gecertificeerd, sterker nog, op 1 juli 2004 waren 125 port facilities ISPS gereed. Dit betekent dat het nieuwe beleid werd uitgevoerd voordat de wetgeving was goedgekeurd. In april 2004 werden de eerste port facilities in Rotterdam gecertificeerd. Dit was vooral om te laten zien hoe goed, hoe veilig en met name hoe snel Rotterdam is. Rotterdam werd de eerste haven ter wereld waar certificaten werden uitgereikt aan port facilities. Deze eerste certificaten werden onder grote belangstelling en in aanwezigheid van de Amerikaanse Minister van Transport door de Nederlandse Minister van Verkeer en Waterstaat en de burgemeester van Rotterdam uitgereikt. Hill ziet anticiperende beleidstoepassing als een bezwaar van de top-down benadering. Niemand, ook de bedrijven in de Rotterdamse haven hebben dit echter ervaren als een negatief punt. Juist de grote belangstelling van de VS was een extra stimulans voor de bedrijven om te zorgen dat ook zij gereed waren voor het certificaat. Een mogelijk probleem zou kunnen zijn dat de voorgestelde wetgeving dusdanig zou worden aangepast dat de uitgereikte certificaten niet meer juist zouden zijn. De kans hierop schat ik klein in. Het was het uitvoeren van Europese en internationale wetgeving, afwijken van deze internationale wetgeving kan eenvoudig niet. Indien de taken, bevoegdheden en verantwoordelijkheden van de actoren zouden veranderen was het relatief eenvoudig om opnieuw certificaten uit te reiken zonder dat daarvoor hele procedures zouden moeten worden gevolgd. De gegevens van gecertificeerde bedrijven worden door het ministerie van Verkeer en Waterstaat doorgegeven aan de IMO die op haar beurt de gegevens publiceert op het internet. Omdat het een dynamische database is, is het relatief eenvoudig gegevens aan te passen.

Het uitgeven van de eerste certificaten vond geen grondslag in de Nederlandse uitvoeringswetgeving. In dit geval is de ISPS code als zodanig als grondslag gebruikt. Door de betrokkenheid van het Havenbedrijf Rotterdam was bekend wat de inhoud van de wetgeving zou gaan zijn, verder was bekend dat de Nederlandse wetgeving zich in een ver gevorderd stadium bevond.

8.6 Managen

Het managen van invoering vindt plaats op drie verschillende niveaus: het managen van beleidsprocessen, het managen van de interne relaties in de organisatie en het managen van externe en interne contacten. Daarnaast worden drie prescriptieve (opleggende) perspectieven van governance (wijze van besturen) onderscheiden: 1) autoritair bestuur: managen door “enforcement” (afdwingen), waarbij de input centraal staat; 2) onderhandelend bestuur: managen gericht op “performance” (resultaat), gericht op output, normen en 3) bestuur door overtuigen: het managen van “co-production” (samenwerking), gericht op de effecten als gezamenlijk resultaat. Invoering vindt theoretisch plaats langs één van deze perspectieven van bestuur. In de praktijk echter kan er sprake zijn van een “uitstapje” naar één van de andere twee perspectieven. Bij een top-down benadering van invoeren, zoals bij de ISPS code het geval was, hoort het perspectief “enforcement”.

Het managen van beleidsprocessen. In de ISPS code en EU regelgeving is sprake van verschillende verantwoordelijkheden, gelieerd aan verschillende rollen [Leidraad Beveiliging, 2003]. In Nederland is volgens de regelgeving de Minister van Verkeer en Waterstaat de zogenaamde Single National Authority, deze kan op zijn beurt voor iedere haven een zogenaamde Competent Authority for Port Security aanwijzen ook wel Designated Authority genoemd. In Nederland zijn dit de burgemeesters vanuit hun betrokkenheid vanuit openbare orde en veiligheid. De burgemeester van Rotterdam laat zich in deze bijstaan door de Port Security Officer (de Havenmeester van Rotterdam).

Het managen van de interne relaties in de organisatie. Zoals ik hiervoor al geschreven heb was het de burgemeester van Rotterdam die de eindverantwoordelijkheid heeft gedragen. Deze burgemeester staat in het algemeen bekend om zijn directieve wijze van bestuur. Hij laat zich adviseren door zijn adviseurs maar hij neemt zelf de beslissingen. In het geval van de ISPS code heeft hij zich laten inspireren en adviseren door de Port Security Policy Board. De taken van de diverse actoren, de vereiste competenties en de benodigde middelen werden vastgelegd in vergaderstukken en plannen. Alles was gericht op het invoeren van de ISPS code en de bijbehorende maatregelen voor 1 juli 2004. Opvallend was wel dat de burgemeester eisen stelde aan de betrokken actoren maar zelf geen middelen beschikbaar stelde. De betrokkenen moesten de middelen, materieel en financieel, uit eigen bronnen beschikbaar stellen. Uiteindelijk zijn de kosten gedragen door het Havenbedrijf Rotterdam, de Douane en de Zeehavenpolitie. Alle drie zijn zij financieel onafhankelijk van de burgemeester. De burgemeester heeft geen afstemming bereikt door samenwerkingsverbanden of management contracten. Het is vooral tight control, de touwtjes in handen willen hebben.

Het managen van externe en interne contacten. De haven van Rotterdam was van 1974 tot en met 2003 de grootste haven ter wereld. Vanuit Rotterdam werd op diverse niveaus' gestreefd dit zo te houden. Rotterdam moest bekend staan als een goede, betrouwbare en veilige haven. Dit botst natuurlijk met het zijn van een goedkope haven. Rotterdam wilde laten zien dat ondanks alle maatregelen er snel en efficiënt gewerkt kon worden. Door het gemeentebestuur en de directies van de betrokken diensten werd op grote schaal de Rotterdamse wijze "verkocht". Het Havenbedrijf Rotterdam heeft het zelf zo weten te regelen dat de in Rotterdam ontworpen toolkit in geheel Nederland gebruikt ging worden. Dit betekende dat de inhoud ten aanzien van procedures en werkwijzen door heel Nederland werd geüniformeerd. Een positieve ontwikkeling. Minder positief is toch wel de invloed die de directie van het Havenbedrijf heeft uitgeoefend op de uitvoering van een aantal taken van het Toetsingsteam. Economische belangen wogen zwaar, soms zwaarder dan de adviezen van het Toetsingsteam. Contact met de bedrijven werd niet alleen door de Toetsingsteamleden onderhouden maar ook door medewerkers van het Havenbedrijf vanuit een service verlenende gedachte. De gevoelens hierover bij de leden van het Toetsingsteam zijn ambivalent. De wijze waarop het Havenbedrijf Rotterdam de bedrijven benaderde was vooral gericht op het behouden van goede contacten waarbij het economische belang voor Rotterdam, of in dit geval het Havenbedrijf Rotterdam, voorop stond. Het leek op een machtsspel; waar de grenzen liggen tussen wat het Toetsingsteam wel of niet goed vond. Ik ben me dat bewust deze opmerking subjectief en moeilijk te onderbouwen is.

Zet ik de uitleg over de operationele activiteiten op een rij dan is het duidelijk dat er sprake was van congruentie. Tevens is duidelijk gewerkt vanuit het perspectief "enforcement", oftewel top-down. Het kan ook bijna niet anders om vanuit dit perspectief te werken om wetgeving, waar niemand op zit te wachten, in te voeren en de bijbehorende maatregelen te treffen. De sense of urgency ontbrak eerst, toch moest de wet worden geïmplementeerd. De beschikbare tijd was minimaal.

8.7 Relaties

Beleid wordt niet uitgevoerd in een wereld die slechts verandering ondergaat door de uitvoering van dit ene beleid, een beleidsveld wordt juist gekenmerkt door vele processen van beleidsuitvoering die er tegelijkertijd op inwerken, zo schreef ik eerder. Er zijn doelgroepen met elk hun eigen wensen en plannen ten aanzien van de verandering in het betreffende beleidsveld.

Een ander probleem of aandachtsveld bij invoering van nieuwe wetgeving zijn de horizontale en verticale relaties. De betrokken actoren kunnen ieder een eigen belang hebben. Lokaal bestuur kan andere belangen hebben dan nationaal bestuur. Ook binnen het lokale bestuur kunnen diensten of afdelingen elk hun eigen belang hebben. Horizontale relaties bij de invoering van de ISPS code zijn de relaties tussen Havenbedrijf Rotterdam, Douane en Zeehavenpolitie. De horizontale relaties kunnen als goed worden bestempeld. Er is veel overleg geweest op diverse niveaus, tussen de directies van de diensten en op uitvoerende niveau. Toch was in de gevoerde gesprekken waar te nemen dat de meerdere petten van het Havenbedrijf Rotterdam kon leiden tot een bepaalde mate van wantrouwen ten aanzien van beslissingen als deze beslissingen dicht tegen commerciële belangen grensden. De diensten hielden door de goede relatie echter de belangen redelijk in balans. Verticale relaties zie ik hier als de relatie tussen het Havenbedrijf Rotterdam en het ministerie van Verkeer en Waterstaat; de relatie tussen de Douane en het ministerie van Financiën en de relatie tussen de Zeehavenpolitie en het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. De belangrijkste verticale relatie was, en is nog steeds, in dit kader de relatie tussen het Havenbedrijf Rotterdam en het ministerie van Verkeer en Waterstaat. De relaties tussen de Zeehavenpolitie en de Douane met hun betreffende ministeries zijn van veel minder groot belang omdat deze twee diensten autonoom van het Ministerie van Verkeer en Waterstaat konden handelen omdat zij andere belangen dienen. De Zeehavenpolitie heeft deelgenomen omdat zij een algemene taak hebben in de handhaving vanuit het strafrecht en vanuit het oogpunt van openbare orde en veiligheid in de regio Rotterdam Rijnmond. De Douane heeft met name vanuit het oogpunt van expertise van de goederenstroom deelgenomen. Zij bezit veel kennis van fiscale wetgeving, accijnzen, opiumwetgeving, etc.. Ten aanzien van de ISPS code bestond er geen relatie met de betreffende ministeries. De ISPS gerelateerde wetgeving was afkomstig van het ministerie van Verkeer en Waterstaat dat een directe relatie heeft met het Havenbedrijf Rotterdam. Deze verticale relatie was een dominante relatie in het geheel. De communicatie vanuit en met de wetgever liep via het Havenbedrijf Rotterdam.

Zoals eerder geschreven zijn er diverse andere projecten in de haven van Rotterdam gaande. Er is veel aandacht voor criminaliteit in de breedste zin van het woord. Mensensmokkel, diefstal van (edele) metalen, fraude, afpersing, etc.. Al deze activiteiten kunnen door of namens terroristische groeperingen geschieden. De (nationale) overheid is dan ook druk bezig met het versterken van de informatiepositie ten aanzien van terrorisme en met het uitbreiden van de politie, inlichtingen en veiligheidsdiensten, ook in de haven. De aanslagen in Madrid hebben geleid tot het besef, dat het tot dan toe veilig geachte Europa ook doelwit kan zijn van een aanslag. Veel bedrijven vonden de te nemen maatregelen dan ook een logische stap, de sense of urgency groeide. Ik wil hierbij wel nuanceren dat het met name gaat over de risicovolle bedrijven. Kleine, laag risico bedrijven, zoals zandoverslag, vonden de te nemen maatregelen overdreven en een onnodige investering.

Twee andere initiatieven die parallel lopen zijn de Amerikaanse initiatieven CSI (Container Security Initiative) en C-TPAT (Customs-Trade Partnership Against Terrorism). Beide initiatieven zijn er op gericht om te voorkomen dat ongewenste goederen of personen naar de VS komen. Deze initiatieven betekenen de komst van nucleaire detectiepoorten, Amerikaanse douaniers in de Rotterdamse haven, beter toezicht op het beladen en behandelen van containers in de gehele supply chain. Al deze maatregelen te samen moeten elkaar versterken.

Als vervolg op de hiervoor genoemde activiteiten ondernamen de bedrijven in de Rotterdamse haven ook zelf allerlei activiteiten. Door samen na te denken over bijvoorbeeld de wijze van het aanleveren van scheepsbenodigdheden, verpakt onder veilige omstandigheden en het garanderen van een veilige wijze van transport trachten deze bedrijven mee te werken aan veiligere haven. Een tweede activiteit door het bedrijfsleven is het ontwikkelen van een toegangkaart met biometrische mogelijkheden om een snelle, maar veilige wijze van controle aan de poort te garanderen.

8.8 Macht

De burgemeester van Rotterdam is door de Minister van Verkeer en Waterstaat benoemd als regionale Havenbeveiligingsautoriteit van Rotterdam Rijnmond. Grondslag hiervoor is de Havenbeveiligingswet. Hij is verantwoordelijk voor de beveiliging van de havens van Rotterdam, Schiedam en Vlaardingen. De burgemeester heeft vervolgens de Havenmeester van Rotterdam aangewezen als de Havenbeveiligingsofficier. Probleem is wel dat de Havenmeester en zijn organisatie deel uitmaken van het Havenbedrijf Rotterdam. Het Havenbedrijf Rotterdam heeft in de Rotterdamse haven een machtspositie. Zij is verantwoordelijk voor de natte en droge infrastructuur, het reguleren van het scheepvaartverkeer, het toekennen van ligplaatsen en is beheerder van de beschikbare grond en kades.

Tijdens het gehele traject van invoering is duidelijk geworden dat de directie van het Havenbedrijf Rotterdam een grote rol heeft gespeeld als het gaat om het behouden van goede relaties met voornamelijk grote bedrijven in de Rotterdamse haven. Deze houding, hoewel verklaarbaar vanuit economisch oogpunt, is een betwistbare houding. Voor ieder bedrijf in de Rotterdamse haven, groot of klein gelden dezelfde regels. Uiteraard wegen economische belangen zwaar, maar deze mogen geen invloed hebben op de maatregelen die dienen te worden uitgevoerd. Proportionaliteit werd door het Toetsingsteam toegepast, dit wil zeggen dat de maatregelen werden afgestemd op de risico's van het bedrijf en de schepen die het ontvangt. Op verschillende manieren is getracht invloed uit te oefenen op het Toetsingsteam door de directie van Havenbedrijf Rotterdam. Dit werd rechtstreeks gedaan of via de Stuurgroep Port Security door onder andere het opleggen van strakke richtlijnen. Bij de Toetsingsteamleden stond integriteit voorop, de onderwerpen zijn bespreekbaar gemaakt binnen de eigen organisaties zodat bespreking in de stuurgroep Port Security mogelijk was.

Het Havenbedrijf Rotterdam maakt deel uit van de Port Security Policy Board, zit in diverse overlegcommissies, is lid van het Toetsingsteam, heeft uiteindelijk een handhavingfunctie gekregen en heeft bovenal grote economische belangen in de haven. Deze meerdere "petten" die het Havenbedrijf draagt heeft enerzijds voor een groot aantal vragen geleid zoals: "kan een commercieel bedrijf wel op deze manier integer handelen?". Anderzijds heeft het Havenbedrijf Rotterdam een flinke stempel kunnen drukken op de nationale wetgeving. Hierdoor was het weer mogelijk om, anticiperend op de komende wetgeving de invoering van de ISPS code snel te laten verlopen. Tevens kon, doordat het Havenbedrijf Rotterdam zo nauw betrokken was bij het maken van het nationale beleid, voorkomen worden dat er sprake was van een groot "implementation gap", het verschil tussen het voorgenomen beleid en de uiteindelijke werking van het beleid.

In het gehele traject is de rol van de burgemeester een hele belangrijke rol. De burgemeester is degene die een besluit neemt om de port facility wel of niet te certificeren. Hij doet dit overigens op advies van de Havenbeveiligingsofficier. De burgemeester is verantwoordelijk voor de openbare orde en veiligheid alsook voor de rampen en calamiteiten bestrijding. De Havenmeester, tevens Havenbeveiligingsofficier, is verantwoordelijk voor de veiligheid in de haven. Hij beschikt hiervoor over de organisatie Rotterdam Port Authority (RPA), een onderdeel van het Havenbedrijf Rotterdam. Zijn formele macht ontleent de burgemeester aan de Havenbeveiligingswet.

Initiator van de ISPS code in Rotterdam is het Regionaal Beleidsoverleg Rampenbestrijding die op haar beurt de Port Security Policy Board heeft ingesteld. De burgemeester laat zich adviseren over port security door dit Port Security Policy Board. Hij laat zich echter vertegenwoordigen door leden van de Algemene Bestuursdienst Rotterdam.

Het bedrijfsleven in de Rotterdamse haven heeft een organisatie die haar belangen behartigt, Deltalinqs. Deze organisatie is door haar grootte en de belangen die zij vertegenwoordigt een belangrijke speler in het machtsspel. Ook op het gebied van port security heeft zij haar steentje bijgedragen, dit gebeurde echter pas in een laat stadium.

8.9 Competenties

Om invoering via top-down wijze te bewerkstelligen moet de betrokken overheid beschikken over medewerkers met de juiste competenties, zeker als de inhoud van de wetgeving nog niet bekend is en invoering van de wetgeving snel dient te geschieden.

Bij de samenstelling van het Toetsingsteam is rekening gehouden met de (eerder verworven) competenties van de leden. Uitgangspunt was een multidisciplinair team samen te stellen uit medewerkers met de volgende kerncompetenties:

- Kennis: minimaal HBO niveau verkregen door studie of interne opleiding, enkele jaren werkervaring in de haven of nautische sector.
- Vaardigheden: contactgerichtheid, overtuigingskracht, flexibiliteit, persoonlijk gedrag, organisatieloyaliteit, integriteit en inzet.

Elk toetsingsteamlid werd geselecteerd door het hoofd van zijn organisatie. De achtergrond van de leden is divers waardoor kennis en kunde werd samengebracht in één team. Het ontbrak echter aan specifieke kennis op het gebied van risicomanagement. Om deze deficiëntie weg te werken is gezamenlijk een opleiding Risicomanagement op HBO niveau gevolgd.

De beleidsmedewerkers bij het Havenbedrijf Rotterdam die landelijk en in Europees verband deelnemen aan werkgroepen en stuurgroepen voldoen aan dezelfde competenties. Hun kennisniveau ligt op Wetenschappelijk niveau.

Niet alleen de overheidsmedewerkers dienen te beschikken over competenties, wettelijk worden ook eisen gesteld aan de personeelsleden van de port facilities die belast zijn met de uitvoering van security maatregelen. Volgens de Wet particuliere beveiligingsorganisaties en recherchebureaus (Wpbr) dienen zij in het bezit te zijn van het certificaat beveiligiger. Volgens de Havenbeveiligingswet dienen zij vervolgens in het bezit te zijn van het aanvullende diploma Havenbeveiligiger. Toezichthouder op Wpbr is de politie.

8.10 Budget

In tegenstelling tot de VS heeft de nationale en lokale overheid in Nederland geen financiële middelen beschikbaar gesteld voor de invoering van de ISPS code of om het bedrijfsleven te ondersteunen bij het nemen van security maatregelen. Opvallend was of is dat de burgemeester eisen stelde aan de betrokken overheidsdiensten en bedrijven maar zelf geen middelen beschikbaar stelde. De betrokkenen moesten de middelen, mensen, materieel en financiën, uit eigen bronnen beschikbaar stellen. Uiteindelijk zijn de kosten voor de ontwikkeling van de toolkit gedragen door het Havenbedrijf Rotterdam. Het Havenbedrijf Rotterdam, de Douane en de Zeehavenpolitie zijn financieel onafhankelijk van de burgemeester, een bijdrage in de kosten was zeker op z'n plaats geweest. De burgemeester heeft geen afstemming bereikt door samenwerkingsverbanden of management contracten. Het is vooral tight control, de touwtjes in handen willen hebben zonder daar zelf een financiële bijdrage voor te hoeven leveren.

Per port facility is door het ministerie van Verkeer en Waterstaat 500 euro beschikbaar gesteld voor het opzetten van een beheersorganisatie door het Havenbedrijf Rotterdam. Het Havenbedrijf heeft deze bijdrage gebruikt als tegemoetkoming in de ontwikkelkosten van de toolkit. Een hulpmiddel waardoor het mogelijk is geworden in Rotterdam en in de overige zeehavens van Nederland de ISPS code tijdig in te voeren, op een uniforme wijze.

Tijdens de invoering en kort na de uitvoering van de ISPS maatregelen heeft geen enkele onderneming bezwaar gemaakt of is in beroep gegaan tegen de opgelegde maatregelen en de bijbehorende investeringen. Dit is opmerkelijk te noemen omdat uit de gehouden enquête van het Toetsingsteam 85 procent van de bedrijven heeft moeten investeren en dit niet begroot had. De genoemde bedragen variëren tussen 40.000 euro en enkele tonnen. Dit kan voortkomen uit het feit dat 70 procent van de

respondenten vindt dat de maatregelen proportioneel zijn met de huidige dreiging van het terrorisme na de aanslagen in de VS. 55 procent denkt dat de opgelegde maatregelen de kans op een terroristische aanslag verkleinen.

8.11 Communicatie

In voorbereiding op de invoering van de ISPS code zijn door het Havenbedrijf Rotterdam voorlichtingsbijeenkomsten georganiseerd. Deze bijeenkomsten vonden eens per zes weken plaats. De opkomst van het aantal Port Facility Security Officers was groot. De teneur tijdens de bijeenkomsten en in de verslagen van de bijeenkomsten, geven aan dat de ondernemingen niet blij waren met de te nemen maatregelen en dat de kosten, investeringen voortkomende uit het nemen van de maatregelen door de nationale overheid moesten worden gedragen. Als dat niet gebeurt zouden de handlingcosts worden verhoogd, gevolg daarvan is dat de Rotterdamse haven te duur wordt. Een groot aantal ondernemingen, waaronder de petrochemie, gaven echter te kennen dat zij al adequate maatregelen hadden genomen. De bezwaren die gemaakt werden zijn vervolgens besproken in de Port Security Policy Board. Een groot container overslag bedrijf heeft hiervan ook daadwerkelijk gebruik gemaakt. Per container die “gehandeld” wordt moet een bedrag worden betaald.

Op een slimme manier is gebruik gemaakt van de toolkit om voorlichting te geven over de vorderingen van de invoering van de Havenbeveiligingswet en de werking van de toolkit met bijbehorende procedures. Daarnaast is gebruik gemaakt van de internetsite van het Havenbedrijf Rotterdam om toelichting te geven op de inhoud van de ISPS code en de Havenbeveiligingswet. De kosten hiervan werden gedragen door het Havenbedrijf Rotterdam.

Door de leden van het Toetsingsteam heeft ook veel “warme” communicatie plaatsgevonden met de bedrijven. Via dit persoonlijk contact is getracht om betrokken te blijven met de port facilities waardoor het bekend was tegen welke problemen de port facilities opliepen. Ook hebben de accountmanagers van het Havenbedrijf Rotterdam veelvuldig contact onderhouden met de port facilities over de voortgang van de te nemen maatregelen, het betrof dan vooral de infrastructurele aanpassingen van het haventerrein of de toegangswegen.

Uit de reacties van de ondernemingen en het uitblijven van bezwaar- en beroepsprocedures wil ik voorzichtig concluderen dat de ondernemingen de wijze van invoeren, top-down, goedkeuren. Volgens mij is dit mede te verklaren uit het gehele traject van communicatie voorafgaande aan de invoering en tijdens de uitvoering van de ISPS code

8.12 Afronding

Als afsluiting van de studie Risicomanagement heeft het Toetsingsteam een scriptie geschreven. Hiervoor is een enquête gehouden onder de verantwoordelijke Port Facility Security Officers (verantwoordelijk voor de beveiliging van de port facility). In totaal zijn 60 enquêteformulieren verzonden, response was 53 procent. Ruim 55 procent van de respondenten gelooft niet dat de Rotterdamse haven een groter doelwit is geworden voor terroristische activiteiten na de terroristische aanslagen in de VS (2001). Bijna 40 procent denkt echter dat de kans op een aanslag groter is geworden. Meer dan 70 procent van de respondenten vindt dat de opgelegde maatregelen vanuit de ISPS code in overeenstemming zijn met de huidige situatie (proportioneel). Dat de security maatregelen bijdragen tot het verkleinen van de kans op een terroristische aanslag gelooft 55 procent. Dat de te nemen security maatregelen geleid tot investeringen wordt aangegeven door bijna 85 procent; het investeringsbedrag was bij 85 procent van de ondernemingen niet opgenomen in de begroting. De communicatie over de ISPS code wordt door de ondernemingen (zeer) gewaardeerd.

Een ander punt was dat niet-conforme uitvoering van de ISPS maatregelen, lang niet altijd te wijten is aan deloyaal of op eigen gedrag gericht gedrag van de uitvoerenden. Het bleek een gevolg te zijn van het handelen van andere actoren in het beleidsveld. Eén van de problemen bij de invoering van de ISPS code, gericht op beveiliging (security), was de kant van de veiligheid (safety). Het volledig

afsluiten van port facilities was in strijd met de veiligheid. Vooral bedrijven die 's nachts niet operationeel zijn maar waar wel schepen liggen afgemeerd komen in strijd met de ARBO wetgeving. Steigers moesten worden voorzien van afsluitbare hekken of afzettingen zodat onbevoegden hier geen gebruik van kunnen maken. Hulpdiensten moeten echter het terrein wel op kunnen komen. Poorten en noodpoorten moesten voorzien van deugdelijk sloten, etc., etc.. Telkenmale dient een afweging te worden gemaakt tussen safety en security. De meeste bedrijven kozen overigens voor security en trachtten alternatieven te bedenken voor de safety.

De invoering van de ISPS code via een top-down wijze heeft gewerkt. Door zijn wijze van bestuur (enforcement) is het de burgemeester van Rotterdam gelukt om door samenwerking van betrokken partijen het onmogelijk geachte doel te behalen, namelijk het invoeren van de ISPS code en het certificeren van de port facilities in de Rotterdamse haven voor 1 juli 2004. Kritiek, conform de punten die Hill heeft genoemd, was er volop. Toch heeft de sense of urgency en de tijdsdruk gewonnen. Dit werd vooral duidelijk na de aanslagen in Madrid, niet alleen de VS is een doelwit voor terroristen.

Vul ik de door mij geschetste tabel in dan krijg ik een samenvatting van de punten:

Policy window		
In Nederland was geen sprake van een Policy window		
Kritiek op		
... aard van het beleid	... onderling verband tussen beleidsformulering en invoeringproces	... de normatieve uitgangspunten
Maatregelen om de VS te beschermen.	Het beste jongetje van de klas.	Er zullen geen aanslagen meer plaats vinden.
Managen van		
... beleidsprocessen	... interne relaties	... externe en interne contacten
Verantwoordelijke autoriteiten aangewezen.	Procedures en instructies vastgelegd.	Voortouw genomen.
Anticiperen op		
... komend beleid	... beleidstoepassing	
Er wordt volop geanticipeerd.	Uitreiken ISPS certificaten.	
Relaties		
... horizontaal	... verticaal	
Goede relaties tussen de uitvoerende diensten, en een bepaalde mate van wantrouwen.	Dominante goede relaties van het Havenbedrijf Rotterdam.	

Duidelijk is geworden dat gewerkt werd vanuit het perspectief "enforcement". Dit blijkt wel uit de resultaten bij de wijze waarop het invoeringproces is gemanaged. De beschrijvingen van hoe de beleidsprocessen, de interne relaties en de externe en interne contacten werden gemanaged komen voort uit "enforcement". Blijkbaar kan het ook niet anders om vanuit dit perspectief te werken om wetgeving, waar niemand in (eerste instantie) op zit te wachten, in te voeren en de bijbehorende maatregelen te treffen. De sense of urgency ontbrak eerst, toch moest de wet binnen korte tijd worden ingevoerd en daar is de medewerking van de overheidsdiensten en de bedrijven in de haven voor nodig. De sense of urgency bij de bedrijven ontstond pas na de bomaanslagen in Madrid. Het kwam allemaal wel heel dichtbij.

In Nederland is geen gebruik gemaakt van een Policy window. Op het moment dat duidelijk werd dat nieuwe wetgeving op komst was werd gewerkt aan nieuwe wetgeving en heeft het Havenbedrijf Rotterdam een bijdrage geleverd en zelfs op diverse fronten het voortouw genomen.

De bezwaren, kritieken, van Hill tegen de top-down benadering van invoeren zijn mij duidelijk en worden door mij onderschreven, zie de genoemde kritieken op de aard van het beleid, het onderlinge verband tussen beleidsformulering en invoeringproces en de normatieve uitgangspunten. De

wetgeving is vooral gericht op de bescherming van de VS, het level playing field in Europa stond onder spanning en het is niet rationeel om te denken dat met het nemen van dit soort maatregelen aanslagen kunnen worden voorkomen. Daar is meer voor nodig.

Toch is de invoering van de ISPS code een succes geworden. Dit succes is volgens mij te verklaren door de wijze waarop geanticipeerd is door het Havenbedrijf Rotterdam op de komende regelgeving en de relaties op horizontaal en verticaal niveau. Zonder de dominante rol van het Havenbedrijf Rotterdam en de betrokkenheid van de diensten in de Rotterdamse haven en de relatie van het Havenbedrijf Rotterdam met het ministerie van Verkeer en Waterstaat was het niet mogelijk geweest de wetgeving op tijd tot stand te brengen, de wetgeving in te voeren en de maatregelen te treffen. De communicatie richting de bedrijven heeft ook een grote rol gespeeld.

Mijn analyse ten aanzien van de centrale begrippen: machtspositie, competenties, budget en communicatie toont aan dat het invoeren volgens een top-down wijze mogelijk is zonder dat de invoering van nieuwe wetgeving beroeps- en bezwaarprocedures met zich meebrengt. Ik stel wel dat dit geldt als voldaan wordt aan de eisen zoals die ik gedefinieerd heb in hoofdstuk twee. Een uitzondering vormt het budget. Budget werd niet door de nationale of lokale overheid toegekend. Blijkbaar zijn de betrokken overheidsdiensten zich bewust van het belang van de in te voeren maatregelen en wilden zij zelf de middelen beschikbaar stellen. Of is het de macht van de huidige burgemeester van Rotterdam?

9. Handhaving, een analyse

9.1 Handhaving in Rotterdam

De Havenmeester, die is aangewezen als verantwoordelijke voor port security in de Rotterdamse haven, maakt deel uit van de directie van het Havenbedrijf. Het grootste deel van de activiteiten van het Havenbedrijf zijn commerciële activiteiten waarbij het maken van winst voorop staat. Het bekendstaan als een veilige haven is belangrijk maar het genereren van inkomsten is voor het Havenbedrijf Rotterdam misschien nog wel belangrijker. Op de werkzaamheden van het bureau Port Security is geen zicht of controle door de overige handhavingdiensten in de haven. Er wordt geen verantwoording afgelegd aan derden, er wordt slechts teruggekoppeld in het Port Security Policy Board. Waar ligt de grens tussen het nog acceptabel vinden en wanneer niet, van vastgestelde gebreken in de beveiligingsmaatregelen als het gaat over één van de grootste overslagbedrijven in de Rotterdamse haven, verantwoordelijk voor het grootste deel van de omzet op het gebied van kolen- en ertsoverslag? Wat als de beveiligingsmaatregelen van de Cruise Terminal niet overeenkomen met de afgesproken maatregelen terwijl het Havenbedrijf Rotterdam en het bestuur van de stad Rotterdam graag de Cruise schepen zien komen vanwege de inkomsten? Ik denk dat het moeilijk is om onafhankelijkheid te blijven garanderen. Vanaf wanneer weegt het commerciële belang zwaarder dan maatregelen om aanslagen te voorkomen als er in Nederland geen aanslag wordt gepleegd? Het Havenbedrijf is zelf eigenaar van een aantal kades, steigers, boeispennen en boeien in de haven en verhuren die aan schepen. Tot voor kort was het Havenbedrijf participant van de Cruise Terminal Rotterdam. Bij de opzet en het handhaven van de beveiligingsmaatregelen van deze genoemde faciliteiten kan de onafhankelijkheid onderwerp van discussie zijn. Tijdens de toetsing van de port facilities waar het Havenbedrijf Rotterdam eigenaar van is, is gekozen om de toetsing te laten plaatsvinden door leden van het Toetsingsteam voortkomende uit de Politie en de Douane. De handhaving en controle van de beveiligingsmaatregelen ligt echter bij het bureau Port Security en de controleurs van het Havenbedrijf. Een mogelijke verstrengeling van belangen en bevoegdheden is hierbij aanwezig.

Jaarlijks dienen de port facilities security oefeningen te houden om te controleren of de voorgestelde maatregelen en procedures ook daadwerkelijk werken. Toezicht op de naleving ontbreekt momenteel. Dat dit nodig is mag duidelijk zijn. Zonder oefening is het niet mogelijk een oordeel te geven over de maatregelen. Het ontbreekt op deze wijze ook aan informatie bij de gemeente Rotterdam over de geoefendheid en “awareness” voor terroristische acties. Essentieel als je een oordeel moet geven over het feit of de Rotterdamse haven goed is beveiligd tegen terroristische acties. De EU is overigens ook voornemens om controles uit gaan (laten) oefenen door een Europees Toetsingsteam. Alleen roepen dat alles veilig is, is dan niet voldoende.

9.1 Macht

In de Havenbeveiligingswet is de rol van de Politie en de Douane niet beschreven als het gaat om handhaving. Deze taak is weggelegd voor wat de wet noemt “de havenautoriteit”. De handhaving van de huidige regels moet worden bereikt met bestuurlijke handhaving in Rotterdam door het Havenbedrijf Rotterdam. Het intrekken van het afgegeven certificaat, een zwaar middel vanuit de bestuurlijke handhaving, zal volgens mij in de praktijk pas gebeuren als uiterste middel. De commerciële belangen voor Rotterdam en het Havenbedrijf Rotterdam zullen hierin een rol spelen. De economische belangen en de concurrentie van andere havens is groot. Hierdoor is het mogelijk dat het werken met twee petten op door de Havenmeester en het Havenbedrijf (publieke én privaat) wel heel erg moeilijk is. Verlies van bedrijven in de haven betekent minder economisch gewin en het directe en indirecte verlies van banen in Rotterdam en omgeving. Mijn stelling is dat een goede balans dient te worden gevonden tussen veiligheid en economie. Te veel van het één leidt tot het verlies van het ander. Veel aandacht voor veiligheid gaat ten koste van de economische belangen, te veel aandacht voor de economische belangen gaat ten koste van de veiligheid. Dit overlaten aan het Havenbedrijf Rotterdam is als het ware de kat op het spek binden. Doordat de betrokkenheid en het toezicht van de

Politie en de Douane minimaal is op de activiteiten van het Havenbedrijf Rotterdam is het niet duidelijk wat er gebeurt of juist niet gebeurt. Op korte termijn moet naar een oplossing worden gezocht.

Vanuit het ministerie van Verkeer en Waterstaat wordt momenteel de mogelijkheid onderzocht om de Douane en de Politie een rol te laten spelen in de handhaving. Hierbij wordt dan een parallel getrokken naar andere wetten zoals de Arbeidsomstandighedenwet en Zeevaartbemanningswet. Hierdoor wordt het mogelijk informatie te delen met de dienst die belast is met de daadwerkelijke handhaving. Volgens mij dient de handhaving van de ISPS code op korte termijn volledig te worden ingebed in de structuur van de Politie en de Douane die vanaf het begin af aan betrokken waren bij de invoering van de ISPS code. Dit moet wettelijk vastgelegd worden. Naast het voorkomen van de reeds eerder genoemde twee petten problematiek van het Havenbedrijf zal de kennis en expertise over de afzonderlijke werkgebieden een belangrijke schakel zijn in het creëren van meer veiligheid. De betrokkenheid van de overheidsdiensten kan kwaliteitsverhogend werken voor de informatiepositie en de informatiehuishouding. Het optreden op basis van adequate risicoanalyses en informatiegestuurde inzet zal bijdragen tot een veiligere haven. Zolang geen formele bevoegdheid, dus macht, ligt bij de Politie en de Douane is het vooral noodzakelijk dat er zicht komt op de activiteiten en resultaten van het bureau Port Security van het Havenbedrijf. Dit kan door het detacheren van een medewerker van Politie of Douane bij het betreffende bureau. Beter zou het zijn de taken van het huidige bureau Port Security neer te leggen bij een speciaal, op te richten bureau Port Security van de gemeente Rotterdam.

9.2 Competenties

In de huidige opzet worden controles uitgevoerd door controleurs gevaarlijke stoffen van het Havenbedrijf Rotterdam. Deze medewerkers beschikken over specialistische kennis en kunde op het gebied van gevaarlijke stoffen, veelal op MBO/HBO niveau. Voor het uitvoeren van de handhavingstaak in het kader van de ISPS code ontvangen zij informatie van de medewerkers van het bureau Port Security van het Havenbedrijf. Omdat zij voorzien van een duidelijke taak, op pad worden gestuurd door bureau Port Security, is additionele kennis of kunde niet nodig. Door het ontbreken van de specifieke kennis op het gebied van security is het niet mogelijk dat zij zelfstandig actie ondernemen op geconstateerde gebreken op het gebied van de ISPS code. Wel spreken zij ter plaatse de Port Facility Security Officer aan, indien aanwezig. De controleurs zijn en blijven afhankelijk van het bureau Port Security die hierdoor haar machtspositie versterkt.

De medewerkers van het bureau Port Security van het Havenbedrijf hebben deelgenomen aan het Toetsingsteam Rotterdam, zij beschikken over de vereiste kerncompetenties.

9.3 Budget

Het Havenbedrijf Rotterdam voert haar wettelijk taak uit binnen de jaarlijkse exploitatiebegroting van het Havenbedrijf Rotterdam. Een extra budget wordt niet toegekend door het ministerie van Verkeer en Waterstaat of door de gemeente Rotterdam. Hierdoor kan het gevaar ontstaan dat security in de haven een minder grote rol gaat spelen in economisch moeilijke tijden. Het zou in dit licht beter zijn een onafhankelijk budget toe te kennen aan het bureau Port Security van het Havenbedrijf Rotterdam

9.4 Communicatie

Door het Havenbedrijf Rotterdam wordt op hun internetsite informatie geboden over de ISPS code, de te nemen maatregelen en over het security level in de haven van Rotterdam. Door de aanwezigheid van de controleurs gevaarlijke stoffen is het mogelijk informele contacten te onderhouden met de beveiligingsfunctionarissen.

De medewerkers van het bureau Port Security onderhouden zowel schriftelijk als telefonisch contacten met de Port Facility Security Officers. Dit doen zij niet alleen naar aanleiding van rapporten van de

controleurs maar ook op basis van het onderhouden van de contacten en het uitwisselen van informatie.

Bijeenkomsten zoals in de invoeringsfase worden niet meer georganiseerd. Een echte noodzaak hiervoor ontbreekt.

9.5 Afronding

Nu de tweede fase, het maken van een Havenbeveiligingsplan, voor de deur staat is het tijd om concrete afspraken te maken over de betrokkenheid en participatie van overheidsdiensten in de Rotterdamse haven. Als te lang gewacht wordt met het nemen van besluiten over de samenstelling en taken, bevoegdheden en verantwoordelijkheden van een Toetsingsteam dan zal het wederom een “haastklus” worden. Toch dient het vooral zo te zijn dat het bestuur van de gemeente Rotterdam het voortouw neemt en de overheidsdiensten zoals Politie, Douane en Koninklijke Marechaussee de uitvoerende diensten moeten zijn. Het Havenbedrijf Rotterdam en de bedrijven in de Rotterdamse haven kunnen een grote bijdrage leveren met hun expertise; zonder hen zal het niet lukken alles op tijd geïmplementeerd te krijgen. Het Havenbedrijf moet echter niet de leiding op zich nemen of krijgen, dit is een taak de burgemeester van Rotterdam of voor een bureau Port Security van de gemeente Rotterdam. Voorkomen moet worden dat de diensten afzonderlijk of in klein comité gaan werken aan allerlei afzonderlijke plannen. Het delen en uitwisselen van informatie zal altijd een moeilijk punt blijven, op grond van de verschillende belangen en bevoegdheden kan niet altijd de informatie worden gedeeld. Zelfs al zou het mogelijk zijn de systemen technisch te koppelen. Toch liggen er mogelijkheden als samenwerking kan worden bewerkstelligd. Ten aanzien van de derde fase ligt het moeilijker. Een groot aantal producenten, vervoerders en afnemers zullen hierin een rol gaan spelen. De branche organisaties en overheidsdiensten zullen hierin elkaar als partner moeten zien te vinden.

De ontwikkelingen die nog staan te wachten, zoals de hiervoor beschreven tweede en derde fase en de invulling van de handhavingstaak vragen om een gedegen en vooral gedragen aanpak. De inzet en betrokkenheid van de overheidsdiensten in de haven, het Havenbedrijf Rotterdam en de bedrijven in de Rotterdamse haven spelen daarbij een belangrijke rol.

Ik zie het oprichten van één bureau Port Security als het belangrijkste alternatief voor de huidige opzet in het kader van de ISPS code én de komende tweede fase. Dit bureau kan zorgen, dat binnen de bestaande bevoegdheden, informatie van de respectievelijke diensten, wordt verzameld en gedeeld. Vergelijk dit met de nationale CT-infobox. Vervolgens kunnen risicoanalyses worden gemaakt, adviezen worden gegeven en audits worden uitgevoerd ten aanzien van (port) security. Het verzamelen en veredelen dient wel te gebeuren door de overheidsdiensten zelf! Het nieuwe bureau Port Security krijgt een coördinerende rol. Deelnemende instanties zouden volgens mij kunnen zijn: gemeente Rotterdam (vanuit het bestuur), Politie Rotterdam (vanuit oogpunt van openbare orde en veiligheid, grensbewaking en inlichtingen), Douane (vanuit fiscale en niet fiscale douanetaken en inlichtingen), Koninklijke Marechaussee (vanuit oogpunt van grensbewaking en inlichtingen), Brandweer (vanuit hun coördinerende rol vanuit rampenbestrijding) en het Havenbedrijf Rotterdam (beheer infrastructuur in de haven). Dit op te richten bureau kan invulling geven aan de komende (twee) fase(n). Het zorgt tevens voor een betere verdeling van de handhavingbevoegdheden. Het gevaar van het werken met twee petten op (commerciële pet en handhavende pet) voor het Havenbedrijf Rotterdam wordt hiermee voorkomen. De huidige taak van het beheer over de ISPS plichtige bedrijven en de toetsing daarvan kan ook bij dit nieuwe bureau komen te liggen. Het bundelen en waarborgen van kennis en expertise op het gebied van (port) security is een vereiste om adequaat te kunnen op treden tegen terrorisme. Het voorkomen van aanslagen is een onmogelijke zaak, het verkleinen van een kans op een aanslag is echter wel mogelijk

10. Samenvatting en conclusie

De doelstelling van mijn afstudeeropdracht is het *beschrijven en analyseren* van de wijze van invoeren van de ISPS code in de Rotterdamse haven aan de hand van de bestaande theorie en empirie. Een tweede doelstelling is het *beschrijven en analyseren* op welke wijze de handhavingsorganisatie in Rotterdam is ingericht en werkt. Dit laatste doe ik aan de hand van de empirie.

De door mij gestelde centrale vraag is: “Op welke wijze heeft introductie van de ISPS code plaatsgevonden in de Rotterdamse haven en hoe vindt handhaving plaats?”. Om deze vraag te beantwoorden heb ik de volgende deelvragen gesteld: 1) waarom is de ISPS code ingevoerd? 2) wat houdt de ISPS code in? 3) op welke wijze is de ISPS code ingevoerd? 4) hoe is de handhaving van de ISPS code in de Rotterdamse haven ingericht?

Als eerste heb ik het theoretische kader geschetst. Vervolgens ben ik overgestapt naar de empirie en heb ik een beschrijving gegeven van terrorisme en de Rotterdamse haven (de achtergrond). Vervolgens heb ik een beschrijving gegeven van de ISPS code en de juridische kaders, de wijze van invoeren en de opzet van de handhaving in Rotterdam. De laatste empirische stap was het analyseren van deze wijze van invoeren en opzet van handhaving. De analyse van de wijze waarop invoering heeft plaatsgevonden heb ik uitgevoerd aan de hand van het beantwoorden van vragen zoals, “Hoe worden processen gemanaged?”, “Welke relaties bestaan er?”, “Hoe is geanticipeerd op nog niet bestaande wetgeving?”, “Wat is de machtspositie van actoren?”, “Beschikken de betrokkenen over de juiste competenties?”, “Was er voldoende budget?” en “Op welke wijze heeft communicatie plaatsgevonden?”. Nu is het punt gekomen om een samenvatting te maken en conclusies te trekken. Daar waar ik dacht dat een aanbeveling mogelijk was heb ik die *cursief* weergegeven.

Terrorisme

Na de aanslagen in de VS, september 2001 is de wereld veranderd. Met name de VS is een offensief, zij noemen het zelf een oorlog, begonnen tegen het terrorisme. Dit beperkt zich niet tot de strijd in of tegen één land. Terroristische groeperingen zijn niet gebonden aan een land, zij bestaan voornamelijk uit netwerken van kleine groepen. Wereldwijd draaien de nationale inlichtingendiensten op volle toeren om inlichtingen in te winnen. In de VS is een nieuwe Minister aangesteld, voor Homeland Security. In Nederland hebben we een Nationaal Coördinator Terrorismebestrijding gekregen, ook op Europees niveau is dit het geval. De overheden proberen meer en meer grip te krijgen op de (nationale) veiligheid tegen terroristische aanslagen. Terrorismen wordt gedefinieerd als: “*Terrorisme is het plegen van of dreigen met op mensenlevens gericht geweld, met als doel maatschappelijke veranderingen te bewerkstelligen of politieke besluitvorming te beïnvloeden*”. De middelen die gebruikt kunnen worden om dit terroristische doel te bereiken zijn zeer verschillend. Het kan gaan om aanslagen op mensen of vitale, cruciale infrastructuur, etc.. Het huidige terrorisme is als een fijnmazig netwerk georganiseerd, niet altijd duidelijk is hoe de lijnen lopen. Met name de ontwikkelingen op het gebied van informatie- en telecommunicatietechnieken geven de moderne terrorist de mogelijkheden om op een relatief simpele manier te communiceren. De aanslagen die terroristen plegen zijn gericht op het ontwrichten van de samenleving; door een massapubliek te treffen wordt getracht om disproportionele angst onder de bevolking te creëren. Het nemen van maatregelen tegen dit soort aanslagen is niet of nauwelijks mogelijk. Het verbeteren van de informatiepositie, het uitwisselen van informatie en de samenwerking tussen de nationale en internationale inlichtingendiensten is een essentiële stap in de strijd tegen het terrorisme. Nationaal, Europese en internationale coördinatie is van groot belang. *Momenteel is de informatie in Rotterdam aanwezig bij de diverse overheidsdiensten zonder dat deze op een adequate wijze informatie uitwisselen. Om te kunnen beschikken op het juiste tijdstip over de juiste informatie is het noodzakelijk om informatie te delen binnen de wettelijke kaders. Hiertoe is het noodzakelijk dat samenwerkingsverbanden in een convenant worden vastgelegd. Participanten kunnen zijn Politie, Douane, Koninklijke Marechaussee en het Havenbedrijf Rotterdam.*

Risico's in de Rotterdamse haven

Het nemen van beveiligingsmaatregelen in een haven als Rotterdam is moeilijk, het plaatsen van één hekwerk met één toegangspoort is onmogelijk. De Rotterdamse haven is een groot gebied met veel vormen van industrie, op- en overslag en de daarvoor benodigde vervoersmodaliteiten. Rotterdam is van groot economisch belang voor Nederland. Vele tonnen goederen bestemd voor de Europese landen komen hier het land binnen. Vele goederen vertrekken naar alle landen ter wereld, veelal ook naar de VS. De potentiële doelen in de Rotterdamse haven zijn: de cruiseterminal en de daar liggende cruise schepen, olieraffinaderijen, olie- en chemicaliënopslag, (petro)chemische bedrijven, passagiersterminals, chemicaliën- en olietankers, gascentrales, elektriciteitscentrales, (chloor)pijpleidingen, alle vervoersmodaliteiten, woonkernen en infrastructuur. In de Rotterdamse haven bestonden al diverse maatregelen op het gebied van safety waarvoor al de benodigde security maatregelen bestaan om te voldoen aan de bestaande wetgeving. Voor het verkrijgen van relevante informatie is het nodig dat alle in de haven aanwezige (overheids) diensten zich bewust zijn van de potentiële doelen en de aanwezigheid van mogelijke terroristen. Het creëren van “oren en ogen” in de haven is voorwaarde om tijdig terroristische activiteiten te onderkennen. Informatie-uitwisseling tussen de (overheids) diensten, binnen de wettelijke mogelijkheden moet mogelijk worden gemaakt.

In de nota Politie in ontwikkeling [2005] wordt gesproken over een *virtueel hekwerk*. De auteurs stellen dat het aangrijpingspunt voor de politie ligt daar, waar de stromen over de infrastructuur een plaats krijgen. *Door op de infrastructuur virtuele toegangspoorten te creëren wordt de veiligheid in gebieden vergroot. Omdat momenteel gewerkt wordt aan de inventarisatie van de vitale infrastructuur en mogelijke scenario's in de Rotterdamse haven, onder andere voor het Havenbeveiligingsplan, moeten de mogelijkheden onderzocht worden op welke plaatsen welke technische middelen mogelijk zijn. Dit is een taak die direct onder verantwoordelijkheid van de burgemeester dient plaats te vinden. Het is zaak om onderzoek niet alleen op droge infrastructuur te richten, ook de toegangswegen via zee, stromen en rivieren moeten deel uitmaken van het plan. Te denken valt onder andere aan onderwater detectiesystemen en radarsystemen om aanlandingen op het strand te detecteren.*

Onder de bedrijven die ISPS plichtig zijn is een enquête gehouden over de mogelijke risico's van een aanslag in de Rotterdamse haven. Bijna de helft van de respondenten geeft aan dat de kans op een aanslag niet groter is dan vóór de aanslagen in de VS. Toch geeft 70 procent van de respondenten aan dat de maatregelen die zij moeten nemen proportioneel zijn met de dreiging. Dit gevoel heeft er mede toe geleid dat de invoering van de ISPS code snel kon verlopen.

ISPS code

In de VS is de angst voor een nieuwe terroristische aanslag groot. Maatregelen die getroffen worden hebben invloed op alle vervoersmodaliteiten, mensen en goederen. Dit betekent dat landen waar goederen of mensen vandaan komen te maken krijgen met maatregelen die moeten voorkomen dat mensen of goederen de VS binnenkomen die aanslagen kunnen plegen. De VS hebben ingezien dat het maken van internationale wetgeving om maatregelen te nemen tegen terrorisme een langdurige zaak is en dat niet alle landen willen meewerken. Eén mogelijkheid om de veiligheid van zeescheepvaart, richting de VS te vergroten was het uitbreiden van reeds bestaande wetgeving. Hiertoe werd de bestaande SOLAS conventie uitgebreid, december 2002, met de zogenaamde ISPS code, International Ship and Port facility Security code. De maatregelen zijn gericht op het voorkomen van aanslagen op een zeeschip, liggend in een haven. Of het schip te gebruiken als middel voor een aanslag. Schepen moeten maatregelen nemen om te voorkomen dat de verkeerde mensen of goederen aan boord komen, die een aanslag willen plegen op of met het schip. Anderzijds moet de port facility, het bedrijf dat het schip ontvangt, maatregelen nemen om te zorgen dat mensen of goederen niet bij schip kunnen komen. Daarnaast moet de ISPS code gaan leiden tot meer uitwisseling van informatie over maritieme veiligheid.

Europa heeft een EU Verordening (Nr. 725/2004, 31 maart 2004) gemaakt om de internationale wetgeving om te zetten naar Europese wetgeving. Deze EU Verordening gaat verder dan de ISPS code; aanbevelingen uit de ISPS code zijn omgezet naar verplichtingen. De nationale overheden moeten vervolgens de EU Verordening omzetten naar nationale wetgeving. In Nederland heeft dit

geresulteerd in de Havenbeveiligingswet. Probleem is de invoeringsdatum geworden. Op 1 juli 2004 was de ISPS code en de EU verordening (wereldwijd) van kracht, de Havenbeveiligingswet pas zes weken later.

In Nederland is de Minister van Verkeer en Waterstaat de verantwoordelijke autoriteit op het gebied van maritieme beveiliging. De Minister heeft een Leidraad opgesteld waaraan port security in Nederland moet voldoen. De Minister heeft vervolgens bevoegdheden geattribueerd aan de burgemeesters van de grote havensteden. De burgemeester van Rotterdam heeft op zijn beurt de uitvoering van de invoering en de handhaving gedelegeerd aan de Havenmeester van Rotterdam die daarmee de functie van Port Security Officer is gaan bekleden. De Havenmeester werkt voor het, verzelfstandigde Havenbedrijf Rotterdam.

Om de plannen en maatregelen die voortkomen uit de ISPS code, te toetsten is in Rotterdam een multidisciplinair ISPS toetsingsteam opgericht. Het team bestond uit medewerkers van het Havenbedrijf Rotterdam, Politie Rotterdam Rijnmond en Douane Rotterdam. Omdat het een samenwerkingsverband was van één private en twee publieke instellingen kon de balans worden gevonden tussen commerciële, economische belangen en publieke verantwoordelijkheden. Ook in de stuurgroep Port Security was deze mix te vinden.

Invoering van de ISPS code

Invoering van beleid is één van de fasen binnen de beleidscyclus. Het volgt op de fase van beleidsbepaling. In de praktijk is het zo dat niet al de fasen uit de beleidscyclus één voor één worden doorlopen. De ene fase start in praktijk al voordat de andere fase volledig is afgerond. Wachten tot het gehele beleid is vastgelegd in wetgeving en van kracht wordt verklaard kan lang duren, tijd die vaak ontbreekt. In eerste instantie ontbrak bij de bedrijven de sense of urgency terwijl het Havenbedrijf Rotterdam en het ministerie van Verkeer en Waterstaat overtuigd waren van de tijdsdruk die zou ontstaan bij de invoering; het betrof immers internationale wetgeving waaraan voldaan diende te worden. Invoering kan op een aantal wijzen plaatsvinden, in de literatuur worden drie hoofdvormen onderscheiden: top-down, bottom-up en de zogenaamde “synthesizers” waarbij door coproductie wordt gekomen tot invoering.

De ISPS code is door de grote tijdsdruk en het ontbreken van bestaande wetgeving op dit gebied als het ware opgelegd, afgedwongen (enforcement) door de overheid zonder al te veel overleg of compromissen. Wel heeft het Havenbedrijf Rotterdam een grote stempel gedrukt op de inhoud van de Nederlandse wet. Deze invloed heeft ze niet gehad bij de totstandkoming van de Europese verordening. Omdat het Havenbedrijf een grote rol heeft gespeeld is het mogelijk geweest een toolkit te ontwikkelen als ondersteuning bij het opstellen van de security plannen. In een vroegtijdig stadium heeft communicatie plaats kunnen vinden naar de betrokken overheidsdiensten en de bedrijven in de haven die moesten gaan voldoen aan de nieuwe eisen. Het Havenbedrijf Rotterdam heeft slim gebruik gemaakt van de mogelijkheden om te participeren in werkgroepen, overleggen en stuurgroepen. Zonder de kennis en inzet van het Havenbedrijf Rotterdam was een snelle totstandkoming van de nieuwe Havenbeveiligingswet moeilijk, zo niet onmogelijk geweest.

De door mij uitgevoerde analyse is gebaseerd op de volgende punten: Policy window, kritieken, procesmanagement, relaties, anticipatie, machtsposities, competenties, budget en communicatie.

1) Policy window:

- a) In Nederland was geen sprake van een Policy window, nationale wetgeving werd pas van kracht na de datum van ingang van de EU Verordening of de IMO wetgeving. De nationale overheid werd gedwongen door het IMO verdrag en de EU Verordening.

2) Kritiek op:

- a) Aard van het beleid: de sense of urgency ontbrak bij de bedrijven in de haven. De maatregelen werden vooral gezien als maatregelen van de VS om hun grens te beschermen.

- b) Onderling verband tussen beleidsformulering en invoering: Nederland wilde het beste jongetje van de klas zijn en had daarmee geen oog meer voor het level-playing field binnen Europa. Invoering was eigenlijk al gestart voordat de wetgeving gereed was.
 - c) De normatieve uitgangspunten: de VS gaan er van uit dat met de invoering van de ISPS code geen aanslagen meer zullen plaats vinden op of door gebruik te maken van zeeschepen in de VS.
- 3) *Het managen van:*
- a) Beleidsprocessen: direct vanaf het begin zijn de verantwoordelijke autoriteiten aangewezen en zijn hun verantwoordelijkheden vastgelegd. Een multidisciplinair toetsingsteam is aangesteld voor de uitvoering van de maatregelen.
 - b) Interne relaties: na aanvang van de invoering zijn alle procedures en instructies vastgelegd in een handboek. De burgemeester heeft besloten dat de benodigde middelen door de drie (overheids) diensten beschikbaar moesten worden gesteld. Ondanks de afstand een “tight control” door de burgemeester van Rotterdam.
 - c) Externe en interne contacten: Rotterdam heeft vanaf het begin het voortouw genomen en heeft haar eigen ideeën “verkocht” in Nederland en Europa.
- 4) *Anticiperen op:*
- a) Komend beleid: vanaf de IMO conferentie waar de plannen voor de nieuwe wetgeving werden gepresenteerd heeft het Havenbedrijf een actieve rol gespeeld. Er werd volop geanticipeerd op datgene dat komen zou.
 - b) Beleidstoepassing: nog voordat de Havenbeveiligingswet van kracht was werden de eerste ISPS certificaten uitgereikt in Rotterdam met het risico dat de wetgeving kon veranderen.
- 5) *Relaties:*
- a) Horizontale relaties: goede relaties tussen de uitvoerende diensten, een bepaalde mate van wantrouwen ten aanzien van de meerdere petten van het Havenbedrijf was aanwezig. Het vinden van een balans tussen de publieke en private taak van het Havenbedrijf werd op deze manier gevonden.
 - b) Verticale relaties: een goede relatie tussen Havenbedrijf Rotterdam en het ministerie van Verkeer en Waterstaat was aanwezig. De dominante rol was weggelegd voor het Havenbedrijf Rotterdam dit uitte zich door een grote mate betrokkenheid van het Havenbedrijf in diverse werkgroepen en bij het tot stand komen van het uiteindelijke beleid.
- 6) *Machtspositie:*
- a) De formele macht bij de invoering van de ISPS code ligt bij de burgemeester van Rotterdam. De burgemeester heeft door zijn wijze van besturen (“enforcement”) en het delegeren van bevoegdheden aan de Havenmeester gezorgd voor een tijdige invoeren van de ISPS code. Het Havenbedrijf heeft een grote invloed gehad bij de totstandkoming van de nationale Havenbeveiligingswet. Ook heeft het management van het Havenbedrijf een sterke rol gespeeld, informele macht. Zij waren vertegenwoordigd in alle belangrijke werkgroepen en stuurgroepen. Zonder de uitoefening van de informele macht was het echter niet mogelijk geweest de ISPS code op een snelle en goede wijze in te voeren. *Voorkomen moet worden dat de Havenmeester die feitelijk met twee petten op werkt te veel macht heeft; risico van, belangenverstrengeling.. De macht moet op een andere wijze worden toebedeeld..*
- 7) *Competenties:*
- a) Alle actoren van het Havenbedrijf Rotterdam en het Toetsingsteam Rotterdam beschikten over de juiste competenties. Kennis van de regelgeving en affiniteit met de haven was volop aanwezig. Allen beschikten over een HBO of WO niveau, verkregen door studie of interne opleidingen. Juist door de uitwisseling van de kennis en kunde en het volgen van een studie risicomangement werd een grote mate van professionaliteit opgebouwd. Kennis en kunde die niet verloren mag gaan. *Het is aan de betrokken diensten te waarborgen dat deze kennis en kunde aanwezig en beschikbaar blijft.*

8) Budget:

- a) De burgemeester van Rotterdam heeft geen budget toegekend aan het Havenbedrijf Rotterdam of het Toetsingsteam Rotterdam om de ISPS code in te voeren. Elke dienst heeft uit eigen budget de mensen en middelen gefinancierd. Het ministerie van Verkeer en Waterstaat heeft uiteindelijk 500 euro per port facility vergoed aan het Havenbedrijf Rotterdam. Het Havenbedrijf Rotterdam heeft dit geld gebruikt ter dekking van de gemaakte kosten voor het ontwikkelen van de toolkit. Met de tweede fase voor de deur is het goed om de huidige opstelling van de burgemeester in deze ter discussie te stellen. Het kan niet zo zijn dat, als het Havenbedrijf Rotterdam geen middelen meer beschikbaar wil stellen voor het bureau Port Security, de handhavingstaak zal worden verwaarloosd. *Omdat de burgemeester van Rotterdam de wettelijke taak heeft de ISPS code in te voeren zal hij moeten bijdragen in de kosten die de betrokken diensten maken.*

9) Communicatie:

- a) Op een actieve wijze heeft communicatie plaatsgevonden door het Havenbedrijf Rotterdam richting de betrokken bedrijven die een port facility hebben in de haven. Door de vele contacten die bestonden tussen de leden van het Toetsingsteam en de verantwoordelijke port facility security officers is het mogelijk geweest om adequaat in te kunnen spelen op de vragen die, vooral in de beginperiode, bij de bedrijven aanwezig waren. De keuze om via de website van het Havenbedrijf informatie te geven is een verstandige keuze. Iedereen kan deze informatie raadplegen.

Bij de invoering is gewerkt vanuit het perspectief “enforcement”, oftewel het opleggen van beleid onder (streng) toezicht, ook wel (tight) control genoemd. Invoering van de ISPS code is een duidelijk voorbeeld van een top-down benadering van invoeren. Het is niet mogelijk om vanuit het bottom-up perspectief te werken als niemand zit te wachten op al die te nemen maatregelen terwijl de tijdsdruk om te voldoen aan nieuwe internationale wetgeving hoog is. Niet voldoen zou immers grote economische gevolgen (kunnen) hebben voor Rotterdam en de omgeving.

De invoering van de ISPS code op gehanteerde wijze is volgens mij een succes geworden. Dit succes is vooral te verklaren door de wijze waarop door het Havenbedrijf Rotterdam geanticipeerd is op de komende regelgeving en de relaties op horizontaal en verticaal niveau. Zonder de betrokkenheid van de diensten in de Rotterdamse haven en de relatie met het ministerie van Verkeer en Waterstaat was het niet mogelijk geweest de wetgeving op tijd tot stand te brengen, de wetgeving in te voeren en de maatregelen te treffen. Communicatie met de bedrijven in de Rotterdamse haven is mede van invloed geweest op het welslagen.

Handhaving van de ISPS code

Invoeren en handhaven van de Havenbeveiligingswet, de ISPS code, is door de burgemeester van Rotterdam overgedragen aan de Port Security Officer, de Havenmeester van Rotterdam. Deze havenautoriteit heeft voor de uit te voeren beheerstaak de beschikking over een bureau Port Security. Dit bureau Port Security voert het beheer over de gegevens van de port facilities. Zij zijn het aanspreekpunt voor de bedrijven in de haven en voor de meldingen van de overheidsdiensten in de haven. Ten aanzien van de handhaving worden op basis van meldingen van overheidsdiensten of op basis van een steekproef controles uitgevoerd door controleurs van het bureau gevaarlijke stoffen van het Havenbedrijf. Deze controleurs zijn belast met toezicht op de milieuwetgeving ten aanzien van gevaarlijke stoffen. Indien tekortkomingen of het niet naleven van de beveiligingsmaatregelen wordt geconstateerd dan worden hiervan meldingen gemaakt aan het bureau Port Security. Als het nodig is worden acties ondernomen of de leden van het Toetsingsteam worden betrokken bij het vinden van een passende oplossing. Als dit niet leidt tot een oplossing kan worden overgegaan tot het geven van een negatief advies aan de burgemeester van Rotterdam door de Port Security Officer. Om economische schade te voorkomen is dit het uiterste middel. De sancties die volgen zijn van bestuursrechtelijke aard.

Jaarlijks dienen de gecertificeerde port facilities security oefeningen te houden en hier verslag van te doen. Niet duidelijk is of en op welke wijze het Havenbedrijf Rotterdam dit handhaaft. *Verstandig zou het zijn om de leden van het Toetsingsteam Rotterdam hierbij aanwezig te laten zijn om een oordeel te kunnen geven over de mate van geoefendheid van het beveiligingspersoneel en de directies van de port facilities. Op deze wijze is het mogelijk inzicht te krijgen in de mate waarin bedrijven in staat zijn om te gaan met mogelijke dreigingen van terroristische acties op hun haven terrein. Dit is van belang om als haven en als gemeente Rotterdam te weten waar je staat als het gaat om de security in de haven.*

Een analyse aan de hand van mijn centrale begrippen:

1) Machtspositie:

- a) *Om ook maar enige schijn van belangenverstrengeling tegen te gaan moet de macht van het Havenbedrijf Rotterdam worden beperkt. De macht behoort te liggen bij de burgemeester op grond van de Leidraad Beveiliging Havens en Port Facilities van het ministerie van Verkeer en Waterstaat waarin staat: “De rechtspersoon of instantie dient in een hiërarchieke relatie te staan tot politie, havenautoriteiten en hulpdiensten en zijn rol dient inpasbaar te zijn in de calamiteiten- rampenbestrijdingplannen”.* Het Havenbedrijf is momenteel nog steeds de grootste, exclusieve, speler in de haven van Rotterdam met veel macht maar heeft geen hiërarchische verhouding met de politie. Omdat het ontbreekt aan zicht op de activiteiten van het bureau Port Security van het Havenbedrijf Rotterdam is niet duidelijk op welke wijze handhaving plaatsvindt. Hooguit kan door de overige diensten in het Port Security Policy Board om een verantwoording worden gevraagd. In het Havenbeveiligingsplan (Port Security Plan) van Rotterdam is de keuze gemaakt de Havenmeester van Rotterdam te benoemen als Port Security Officer met de volgende motivering: “Vergelijkbaar met zijn taken binnen de nautische verantwoordelijkheden, is de Havenmeester de meest geschikte functionaris om zowel de beheerstaken als operationele taken met betrekking tot havenveiligheid vorm te geven. Veel van deze taken liggen immers in het verlengde van zijn verantwoordelijkheden en bevoegdheden als Havenmeester. Het apparaat (zowel werknemers als infrastructuur) dat de Havenmeester in zijn functie als hoofd van de Rotterdam Port Authority (RPA) ter beschikking staat, gebruikt hij tevens om de functie van Havenbeveiligingsofficier uit te kunnen voeren”. Ik heb sterk het vermoeden dat het Havenbedrijf een grote rol heeft gespeeld bij de totstandkoming van het Havenbeveiligingsplan van Rotterdam.

2) Competenties:

- a) Controle op de handhaving gebeurt door controleurs gevaarlijke stoffen van het Havenbedrijf Rotterdam; op aansturing van de medewerkers van bureau Port Security. De controleurs beschikken over competenties op het gebied van gevaarlijks stoffen en veiligheid (safety). Door de ervaring die zij gedurende het laatste jaar hebben opgedaan ten aanzien van security hebben zij kennis hiervan opgedaan.

3) Budget:

- a) Het Havenbedrijf is een verzelfstandigd overheidsorgaan met een eigen budget. Door de gemeente Rotterdam of het ministerie van Verkeer en Waterstaat wordt geen extra budget toegekend aan het Havenbedrijf Rotterdam. *Om te voorkomen dat port security afhankelijk wordt van alleen de beschikbare financiële middelen van het Havenbedrijf dient het budget door het ministerie van Verkeer en Waterstaat of door de gemeente Rotterdam beschikbaar te worden gesteld.*

4) Communicatie:

- a) Bij de invoering van de ISPS code is veelvuldig gecommuniceerd met de bedrijven, ook nu is het nodig om periodiek de bedrijven te blijven informeren over de huidige stand van beveiliging en om de mogelijke plannen over de tweede fase te communiceren.

Nieuwe wetgeving of regelgeving is weer op komst. In totaal zijn drie fasen onderscheiden: de beveiliging gericht op de schepen (ISPS code), de beveiliging van de haven als geheel (inclusief

infrastructuur) en de beveiliging van de logistieke keten. Het Havenbedrijf Rotterdam houdt zich ook bezig met de komende twee fasen, het is duidelijk zichtbaar dat zij aan de touwtjes blijven trekken en hun invloed daartoe aanwenden. Het is in dit geval niet het bureau Port Security van de Havenmeester maar de strategische beleidsmedewerkers die hun invloed uitoefenen in (werk)groepen. Regionaal zijn de vitale objecten en infrastructuur al door een werkgroep geïnventariseerd. Deze werkgroep bestaat uit het Havenbedrijf Rotterdam, Politie Rotterdam Rijnmond, Gemeente Rotterdam en Douane Rotterdam. Landelijk heeft TNO overigens een vergelijkbare inventarisatie gemaakt. Hoe en op welke wijze de tweede fase wordt vastgelegd in nationale en Europese wetgeving en hoe uitvoering wordt gegeven aan de invoering is nog niet duidelijk. Duidelijk is wel dat ook nu weer wordt geanticipeerd op de totstandkoming van wetgeving. Mogelijk zal top-down invoering weer aan de orde zijn, het zijn vooral (semi)publieke objecten. Om niet verzeild te geraken in de discussie over belangenverstrengeling moet het niet het Havenbedrijf Rotterdam zijn dat de “lead” neemt in deze fase. Zij zijn veelal ook eigenaar van de natte en droge infrastructuur in de haven, hun kennis is overigens onmisbaar.

Met de komst van de tweede fase en de daarvoor benodigde invoering van nieuwe wetgeving is het goed om na te denken over de opzet en inrichting van een organisatie die in Rotterdam adequaat kan optreden en mede invulling kan geven aan de invoering van de nieuwe wetgeving. Ook zouden zij uitvoering kunnen geven aan de handhavingstaak voortkomende uit de ISPS code. Het delen van informatie op het gebied van de beveiliging van de Rotterdamse haven is van belang om op tijd te signaleren waar de risico's liggen. Het gaat dan vooral om een coördinerende rol omdat het delen van informatie wettelijk gezien een moeilijke zaak is. Een ieder heeft zijn eigen taken met bijbehorende bevoegdheden, het verzamelen van informatie hoort dan ook thuis bij de afzonderlijke diensten. Vanuit dit standpunt is het oprichten van één bureau Port Security Rotterdam een mogelijkheid. De leiding berust bij de burgemeester van Rotterdam. Deelnemers zijn: gemeente Rotterdam (vanuit het bestuur), Politie Rotterdam Rijnmond (vanuit oogpunt van openbare orde en veiligheid, grensbewaking en inlichtingen), Douane (vanuit fiscale en niet fiscale douanetaken en inlichtingen), Koninklijke Marechaussee (vanuit oogpunt van grensbewaking en inlichtingen), Brandweer (vanuit hun coördinerende rol vanuit rampenbestrijding) en het Havenbedrijf Rotterdam (beheer infrastructuur in de haven). De taken zijn omvangrijk en liggen op het vlak van: 1) beleidsbepaling, 2) informatieveredeling en analyse, 3) toetsing en 4) de beheerstaken die hiermee gemoeid zijn. Een flinke investering; maar als security en het voorkomen van terroristische aanslagen in of rond de haven belangrijk zijn, dan moet de wil om hierin te investeren ook aanwezig zijn.

Als echter de toezichthoudende taak op de activiteiten van het Havenbedrijf Rotterdam, in het bijzonder die van het bureau Port Security van de Havenmeester, door de Rekenkamer van Rotterdam wordt uitgevoerd is het mogelijk de huidige constructie voort te zetten. Voorwaarde om gebruikt te maken van de aanwezige informatie bij politie en douane is dat deze twee diensten elk bijvoorbeeld een medewerker detacheren bij het Havenbedrijf Rotterdam. Een andere voorwaarde is een grotere betrokkenheid van de gemeente Rotterdam. De taken, bevoegdheden en verantwoordelijkheden dienen op een juiste wijze te worden verdeeld over de autoriteiten.

Overwogen kan worden om een “denktank” port security Rotterdam op te richten waarin de overheidsdiensten, het Havenbedrijf Rotterdam, het Bedrijfsleven en deskundigen (universiteiten) zijn vertegenwoordigd. Een vertegenwoordiger van de AIVD of de MIVD zou hierbij een goede aanvulling zijn.

De mogelijkheden van de door mij genoemde opties en andere mogelijkheden zijn een interessant onderwerp voor een vervolgstudie naar de inrichting van port security in Rotterdam of zelfs nationaal. Hierbij zou kunnen worden aangesloten bij lopende onderzoeken naar de security van de logistieke keten.

Literatuuroverzicht

- Algemene Inlichtingen- en Veiligheidsdiensten, *Jaarverslag 2003*, 2004. Ministerie van Binnenlandse Zaken, Den Haag
- Binnenlandse Veiligheidsdienst, *Terrorisme aan het begin van de 21^e eeuw: Dreigingsbeeld en positionering BVD*, 2001, Ministerie van Binnenlandse Zaken, Den Haag
- Brief van 25 mei 2004 (kamerstukken 29468, nr. 8 vergaderjaar 2003 –2004)
- Brinkman, E., in een interview in *Vrij Nederland*, april 1984
- Derksen, W., *Het college Beleidsprocessen*, 2002
- Dubois, N.L., Duintjer, J.E., Dongen, J.H.G. van, Botbijn, A., Slegtenhorst, R.J.W., Lensen, J.H., Gunst, R.J.M., scriptie voor de opleiding Basis Risicomanagement, *Toegankelijkheid en toetsing. Is met een Toetsingsteam de haven open te houden en toch goed te beveiligen?*, 2004, Rotterdam
- Graaf, H., van de, Hoppe, R., *Beleid en politiek. Een inleiding tot de beleidswetenschap en de beleidkunde*, 1996, Bussum
- Gunsteren, H., van, *Gevaarlijk veilig, terreurbestrijding in de democratie*, 2004, Amsterdam
- Hill, M. en Hupe P., *Implementing Public Policy*, 2002, Londen
- Hill, M., *The Public Policy Process*, fourth edition, 2005, Londen
- International Maritime Organization, *ISPS code, 2003 Edition*, 2003, London
- Kamerstukken II, 2000/01, 27 831, nr. 1 bladzijde 6
- Kernteam Rotterdam-Rijnmond & COT Instituut voor Veiligheids- en Crisismanagement, *Criminaliteitsbeeld Rotterdamse haven*, 2002, Rotterdam
- Kingdon, John W., *Agendas, Alternatives, and Public Policies*, second edition, 2003, Michigan
- Muller E.R., Spaaij R.F.J., Ruitenbergh A.G.W., *Trends in terrorisme*, 2003, COT Instituut voor Veiligheids- en Crisismanagement, Alphen aan de Rijn
- Nationaal Coördinator Terrorismebestrijding, brief aan de Tweede Kamer, *Terrorismebestrijding*, 10 september 2004
- Peper, A., *Na 11 september 2001: veiligheid als schaars goed?*, 2004, in: *Veiligheid, studies over inhoud, organisatie en maatregelen*, 2004, Kluwer
- Pressman, J.L. en Wildavsky, A., *Implementation, how great expectations in Washington are dashed in Oakland; or, why it's amazing that federal programs work at all, this being an saga of te economic development administration as told by two sympathetic observers who seek to build morals on a foundation of ruined hopes*, third edition, 1984, Berkeley
- Projectgroep Visie op de politiefunctie, Raad van Hoofdcommissarissen, *Politie in ontwikkeling, visie op de politiefunctie*, 2005, Den Haag
- Werkgroep Security Zeehavens en Port Facilities, *Leidraad Beveiliging Havens en Port Facilities*, 2003

