Beveiliging in de haven van Antwerpen

Een bedrijfseconomische analyse

Shana HOES

promotor :
Prof. dr. Frank WITLOX

Eindverhandeling voorgedragen tot het bekomen van de graad
Handelsingenieur major operationeel management en logistiek

universiteit hasselt

Woord vooraf

Het kiezen van een onderwerp voor mijn eindverhandeling was niet moeilijk. Ik wist tamelijk snel dat ik mij wou verdiepen in een onderwerp dat zich afspeelde in de maritieme sector. Het uiteindelijke onderwerp was snel gekozen, namelijk beveiliging in de haven van Antwerpen. Dit onderwerp werd behandeld in de cursus vervoersbeleid en ik heb er ook een colloquium over bijgewoond. Het hele beveiligingsgebeuren intrigeerde mij en ik wou er graag meer over te weten komen. Nu ben ik blij dat ik mij een jaar heb kunnen verdiepen in het onderwerp. Door mij bezig te houden met deze eindverhandeling heb ik immers beseft dat ik verder wil in de maritieme sector. Ik kan met andere woorden zeggen dat mijn eindverhandeling mijn keuze om nog een jaar te gaan studeren mee bepaald heeft.

Aanvankelijk leek het schrijven van mijn thesis een simpele opdracht. Ik zou de theorie doornemen en dan de praktijk bestuderen. Maar dit bleek helemaal niet te kloppen. De wetteksten waren vrij technisch en voor een leek was het niet eenvoudig om er de hoofdlijnen in terug te vinden. Daarnaast bleek er een groot verschil te bestaan tussen de theorie en de praktijk. Deze ‘hinderpalen’ hebben het onderwerp nog interessanter gemaakt en het gaf ook een enorme stimulans om het onderwerp onder de knie te krijgen. Volgens mij is dit ook wel gelukt, maar zoals bij alles zal er nog veel veranderen en het is aan mij om deze wijzigingen op te volgen.

Ik wil heel graag Prof. Dr. Frank Witlox bedanken omdat hij mij de mogelijkheid heeft gegeven dit onderwerp uit te werken. Ik wil hem ook bedanken voor het nalezen en verbeteren van mijn teksten. Verder wil ik Dhr. Dominique Cant bedanken omdat hij mij heeft laten proeven van de praktijk. Zonder hem zou ik de ‘vertaalslag’ van theorie naar praktijk nooit hebben kunnen maken. Ik wil hem ook bedanken voor het nalezen en verbeteren van mijn teksten, alsook voor zijn opbouwende kritiek op mijn teksten. Ook bedank ik heel graag mijn ouders voor de hulp en steun. Zonder hen was ik deze vijf jaar niet zo zorgeloos doorgekomen als nu het geval is geweest. Ik wil hen bedanken voor de mogelijkheden die ze mij gegeven hebben en die ze mij nog zullen bieden in de toekomst. Zonder de steun van deze mensen zou deze eindverhandeling niet tot stand zijn gekomen.

Samenvatting

Sinds de aanslagen van elf september 2001 op de WTC-torens in New York is er veel veranderd. Ook de transportsector is hier door beïnvloed en heeft tal van extra beveiligingsmaatregelen moeten invoeren. Het werd immers op 9/11 duidelijk dat terroristen via de transportsector het benodigde materiaal kunnen versturen, alsook aanslagen kunnen plegen met transportmiddelen en op die manier delen van een land kunnen lam leggen. In de Verenigde Staten werd vrij snel het initiatief genomen om de sector een aantal verplichtingen op te leggen om op die manier te proberen terroristische acties te verhinderen en te vermijden.

De maritieme sector reageerde heel snel op de gebeurtenissen van elf september 2001. De IMO (International Maritime Organisation) begon al in november 2001 met de aanpassing van de beveiligingsmaatregelen. In december 2002 organiseerde de IMO een conferentie waar de ISPS-code (een aanvulling op het bestaande SOLAS-verdrag) het resultaat van was. De bedoeling van deze code is het beveiligen van schepen en havenfaciliteiten tegen terroristische aanslagen. Deze code werd aangenomen door de 148 landen verbonden aan het SOLAS-verdrag en moest ingevoerd zijn vóór één juli 2004. De code omvat een aantal voorschriften, een deel A met verplichtingen en een deel B met richtsnoeren. In Europa werd de ISPS-code verankerd in Verordening 725/2004 en om meer uniformiteit te garanderen werden een aantal richtsnoeren uit deel B verplichtend gemaakt. In België werd op 15 juni 2004 een Koninklijk Besluit uitgevaardigd tot oprichting van een federaal comité en lokale comités voor de beveiliging van de havenfaciliteiten. Op dit ogenblik is de overheid aan het werken aan een wetsvoorstel betreffende de maritieme beveiliging.

De belangrijkste verplichtingen die de ISPS-code aan de havenfaciliteiten oplegt zijn de uitwerking van een risicoanalyse, het opstellen van een veiligheidsplan en het aanstellen van een veiligheidsbeambte. Elke havenfaciliteit moet maatregelen uitwerken om de beveiliging van de havenfaciliteit in alle mogelijke omstandigheden te garanderen. Volgens voorschrift 10.3 van Verordening 725/2004 is het aan de verdragsluitende staten om aan te geven welke maatregelen de havenfaciliteiten dienen op te nemen in het veiligheidsplan. In België zijn hiervoor de zogenaamde ‘sjablonen’ uitgegeven. In de haven van Antwerpen is gewerkt met

de ‘Toolkit’ om het uitvoeren van een risicoanalyse en het opstellen van een veiligheidsplan eenvoudiger maken.

Verder moeten de havenfaciliteiten elk jaar een aantal oefeningen houden om na te gaan of het plan in de realiteit uitgevoerd kan worden en doeltreffend is. Deze oefeningen zijn ook nodig om de handhaving van de beveiligingsmaatregelen te garanderen. Niet alleen de oefeningen zorgen voor het op punt houden van de maatregelen, maar ook een goede toegangscontrole is vereist. In de haven van Antwerpen wordt gewerkt met de Alfapass om een goed systeem van toegangscontrole te garanderen.

De havenfaciliteiten zorgen dus enerzijds zelf voor het naleven van de ISPS-code, maar er zijn anderzijds ook externe controles mogelijk door de Europese Commissie of door de nationale autoriteiten die hiervoor bevoegd verklaard zijn.

De invoering van al deze beveiligingsmaatregelen brengt een aantal investeringskosten met zich mee. De Europese Commissie heeft nog geen studie laten uitvoeren naar de financiële kant van het hele beveiligingsgebeuren. De OECD (Organisation for Economic Co-operation and Development) heeft dit wel gedaan en deze studie verschilt op een aantal punten met de praktijk. Verder hebben de havenfaciliteiten een beveiligingstoeslag in het leven geroepen om de kosten van de beveiliging te dekken. Er wordt nagegaan of dit juridisch gezien wel mogelijk is. Daarnaast wordt bekeken wat de mogelijkheden zijn om de kosten terug te winnen via een verhoging van de havengelden of om overheidssteun te krijgen.

Naast de opgelegde verplichtingen aan de havenfaciliteiten, is de ISPS-code ook van toepassing op schepen. Elk schip moet een veiligheidsplan opstellen en een veiligheidsbeambte in dienst nemen. Daarnaast zijn er nog maatregelen die een schip moet uitvoeren om in overeenstemming te zijn met de ISPS-code. Er zijn ook procedures voorzien om de veiligheidsniveaus van een schip en een havenfaciliteit op hetzelfde niveau te brengen indien dit niet het geval zou zijn.

Het is echter niet gebleven bij de ISPS-code. Er zijn nog tal van andere beveiligingsinitiatieven genomen. De meeste initiatieven zijn afkomstig van de Verenigde Staten, maar ook andere partijen eisen verdere maatregelen. Iedereen beseft immers dat de transportketen een doelwit kan vormen en een aanval op de logistieke keten kan heel veel schade veroorzaken. Met de verschillende initiatieven wordt getracht dit risico zo veel mogelijk te beperken.

Inhoudsopgave

Bijlagen

Bijlage 1: Interessante links

Bijlage 2: Contactgegevens van organisaties die opleidingen aanbieden

Hoofdstuk 1: Probleemstelling

1.1 Kader

Sinds de aanslagen van elf september 2001 in de Verenigde Staten van Amerika is er veel veranderd. Alle landen beseffen sinds die dag dat terreur niet duidelijk gedefinieerd kan worden. De leden van de terreurgroepen bevinden zich in verschillende landen en worden al dan niet beschermd door de regeringen van deze landen. Vandaag de dag proberen veel overheden de strijd aan te gaan tegen het terrorisme, denk hierbij aan de oorlog tegen het terrorisme van de Verenigde Staten.

De aandacht voor deze problematiek is eveneens enorm toegenomen binnen de maritieme sector. Een terroristische aanslag op het transportsysteem van een land kan immers grote gevolgen hebben voor de economie. Hierdoor heeft de Internationale Maritieme Organisatie (IMO) in minder dan één jaar tijd de International Ship and Port facility Security code (vanaf nu afgekort ISPS-code) opgesteld als een annex van het SOLAS-verdrag (Safety of Life at Sea: internationale conventie voor de veiligheid van leven op zee). In december 2002 werd deze code goedgekeurd door de IMO-lidstaten. De lidstaten moesten zich tegen één juli 2004 in orde stellen met de verplichtingen van de ISPS-code.

Het doel van deze ISPS-code is te zorgen voor een beter besef van beveiliging binnen de gehele maritieme organisatie. Er moet zowel op de schepen als binnen de havenfaciliteiten een cultuur ontwikkeld worden die gericht is op beveiliging tegen terroristische acties. Aangezien deze ISPS-code deel uitmaakt van het internationale SOLAS-verdrag is het uiteraard verplichtend. De ISPS-code bestaat uit twee delen: een A-gedeelte met verplichtingen en een B-gedeelte met aanbevelingen.

Naast het aannemen van de ISPS-code heeft de IMO op 12 december 2002 de SOLAS-conventie aangevuld met een nieuw hoofdstuk getiteld ‘Special measures to enhance maritime security’, naast het bestaande hoofdstuk met als titel ‘Special measures to enhance maritime safety’. Het laatste begrip duidt op de veiligheid van schepen, en behandelt dus de belangen

van opvarenden. Met het begrip ‘maritime security’ (maritieme beveiliging) wordt verwezen naar de specifieke maatregelen die terroristische aanslagen en andere criminele daden moeten vermijden.

De Europese Unie heeft de ISPS-code overgenomen in een Verordening, namelijk Verordening 725/2004 betreffende de verbetering van de beveiliging van schepen en havenfaciliteiten. De belangrijkste punten van deze verordening kunnen als volgt worden samengevat: (Jacobs en Heuvelman, 2005)

- Het verplicht maken van sommige maatregelen die thans als aanbevelingen staan opgenomen in de ISPS-code. (Men kan dus stellen dat de Europese Verordening iets strenger is dan de ISPS-code zelf.)
- Het verplicht installeren van een nationale autoriteit in iedere lidstaat die verantwoordelijk is voor de beveiliging van het schip en de haveninstallaties.
- Het voorzien van een inspectieproces gesuperviseerd door de Europese Commissie om deze nationale autoriteit te controleren.
- Het uitbreiden van de rol van het opgerichte Maritiem Veiligheidsagentschap (EMSA).
- Het uitbreiden van hoofdstuk XI van de SOLAS-conventie naar een groter aantal scheepstypes.

De bedoeling van deze maatregelen is de volgende:

- Garanderen van een voldoende niveau van veiligheid in de verschillende havens op Europees niveau.
- Verzekeren van een geharmoniseerde implementatie van initiatieven ter beveiliging van de havens binnen de Europese Unie, zodat er geen verschillen zijn voor havengebruikers.
- Verzekeren dat de verschillende maatregelen zo ver mogelijk worden geïmplementeerd, met een maximum veiligheid als resultaat en een minimum aan bijkomende last voor de havens zelf.

Deze verordening werd van kracht op 1 juli 2004 en moet door de lidstaten van de Europese Unie niet eerst worden omgezet naar nationale wetgeving.

In België werd deze ISPS-code verankerd in het Koninklijk Besluit van 15 juni 2004 tot oprichting van een federaal comité en lokale comités voor de beveiliging van de havenfaciliteiten.

Op 2 juli 2004 waren de meeste van de meer dan tachtig Antwerpse terminals in regel met de nieuwe beveiligingsmaatregelen. Dit werd bevestigd door de federale overheid op de ministerraad van 25 juni 2004. Deze goedkeuring werd gegeven op basis van het advies van het federaal comité, op basis van de plannen van de haventerminals en inspecties ter plekke door de lokale comités. De terminals die goedgekeurd werden, zijn toegevoegd aan de 'whitelist' van de IMO. Deze 'whitelist' kan geraadpleegd worden op de website http://gisis.imo.org/Public/ (geraadpleegd op 6 april 2006).

1.2 Het onderzoeksprobleem

De invoering van deze beveiligingsmaatregelen heeft de nodige vragen doen rijzen, ook in de haven van Antwerpen. Er zijn verschillende partijen betrokken bij de invoering van de ISPS-code. Enerzijds kreeg België als verdragsluitende staat de nodige verantwoordelijkheden opgelegd, maar ook de schepen en de havenfaciliteiten moesten zich in regel stellen met een aantal opgelegde verplichtingen. De vraag die zich dan opdringt, is op welke manier elke partij zich het best kon confirmeren met de verplichtingen. De ISPS-code geeft wel een aantal richtlijnen aan, maar het is natuurlijk aan elke partij zelf om ervoor te zorgen dat de beveiligingsmaatregelen getroffen worden. Elke partij moest bovendien rekening houden met de vooropgestelde deadline van 1 juli 2004. De ISPS-code moest ingevoerd worden tegen deze datum. Om alle verplichtingen na te leven, zal de overheid een aantal investeringen moeten doen. Ook de schepen en de havenfaciliteiten zullen bepaalde investeringen moeten uitvoeren. Hierdoor ontstaat de vraag of elke betrokken partij zelf moet instaan voor de kosten of dat het mogelijk is om overheidssteun te krijgen. Op dit ogenblik is er in België geen

sprake van overheidssteun. Als dit er in de toekomst wel zou komen, dan moet er onderzocht worden of de overheidssteun in regel is met de bestaande wetgeving omtrent steunmaatregelen. Als de havenfaciliteiten zelf instaan voor de kosten, kunnen zij deze terugwinnen door een doorrekening in de vrachtprijzen. Deze manier wordt momenteel gehanteerd en vormt juridisch gezien geen enkel probleem. Als de havenbesturen kosten maken, kunnen zij deze recupereren via een verhoging van de havengelden. Ook hier moet gekeken worden naar de juridische kant en nagegaan worden of de heffing niet in strijd is met de regelgeving. Een andere vraag die zich stelt, is hoe de verschillende betrokkenen zullen toezien op de handhaving van de beveiligingsmaatregelen. Het is immers niet de bedoeling om de maatregelen in te voeren en er daarna niet meer naar om te kijken. Er zal moeten gezocht worden naar effectieve manieren om steeds te garanderen dat er voldoende beveiliging is. Naast deze handhaving zullen er ook controles ingesteld moeten worden. Het is aan België als verdragsluitende staat om te bepalen welke mensen hiervoor bevoegd zullen worden.

1.3 Doelstelling

De bedoeling van mijn thesis is om te beschrijven hoe de invoering van de ISPS-code verlopen is in de haven van Antwerpen. Daarnaast wil ik nagaan in hoeverre de getroffen maatregelen gecontroleerd en gehandhaafd worden. Om de theorie om te zetten naar de praktijk zal ik samenwerken met P&O Ports om na te gaan hoe de invoering in werkelijkheid verlopen is. Er wordt tevens bekeken hoe er bij P&O Ports gecontroleerd wordt en tenslotte hoe P&O Ports probeert de beveiligingsmaatregelen te handhaven.

1.4 Centrale vragen

De centrale vragen van mijn thesis zijn:
Hoe gebeurde de invoering van de ISPS-code in de Antwerpse haven, en hoe verloopt de handhaving?

1.5 Deelvragen

Een aantal deelvragen zijn:

1. Wat houdt de ISPS-code in?
   Een duidelijke beschrijving van de inhoud van de code geven. Wat is het toepassingsgebied van de code? Wat zijn de belangrijkste maatregelen die moeten ingevoerd worden? Hoe zit het met verantwoordelijkheden?

2. Op welke wijze werd de ISPS-code ingevoerd in België?
   Hoe werd de ISPS-code in België verankerd in nationale wetgeving? Welke partijen hebben welke verantwoordelijkheden gekregen? Komt de theorie overeen met de praktijk? Hoe is het hele proces verlopen bij de havenfaciliteit P&O Ports?

3. Hoe verloopt de handhaving van de ISPS-code?
   Hoe wordt er gecontroleerd of de maatregelen nageleefd worden? Wie is hier verantwoordelijk voor? Op welke manier zorgt P&O Ports voor het handhaven van de beveiligingsmaatregelen?

4. Wat kost de ISPS-code?
   Wat zijn de algemene kosten van de ISPS-code? Klopt de theorie hiervan met de praktijk?

5. Hoe zit het met de juridische kant van de ISPS-code?
   Kunnen havenfaciliteiten financiële steun krijgen? Kunnen de kosten van de beveiliging doorgerekend worden aan andere partijen?

6. Welke andere initiatieven zijn er naast de ISPS-code?
   Een beschrijving geven van de andere initiatieven en aangeven welke partij de aanzet heeft gegeven tot het initiatief.

Hoofdstuk 2: International Ship and Port facility Security code (ISPS-code)

2.1 De ISPS-code

Tijdens een conferentie van 9 tot 13 december 2002 heeft de IMO (International Maritime Organisation) een aantal wijzigingen aangenomen op het bestaande SOLAS-verdrag (Safety of Life at Sea) van 1974, meer bepaald in hoofdstuk XI-2 waarin dwingende voorschriften (ISPS-code – deel A) en vormende aanbevelingen (ISPS-code – deel B) werden opgenomen. Deze maatregelen zijn gericht op het versterken van de maritieme veiligheid en tevens het voorkomen en onderdrukken van terroristische daden tegen de scheepvaart. Deze aanvulling op het SOLAS-verdrag is de zogenaamde ISPS-code die wereldwijd van kracht werd op 1 juli 2004. De ISPS-code werd door de Europese Commissie omgezet in een Europese wetgeving door de Verordening 725/2004 van 31 maart 2004. Deze Verordening is rechtstreeks toepasbaar in elke lidstaat van de Europese Gemeenschap en bindend in al zijn onderdelen. In deze Verordening werden bovendien enkele richtsnoeren van de ISPS-code (deel B) verplichtend gemaakt.

De doelstellingen van de ISPS-code kunnen als volgt worden samengevat: (www.portofamsterdam.com)

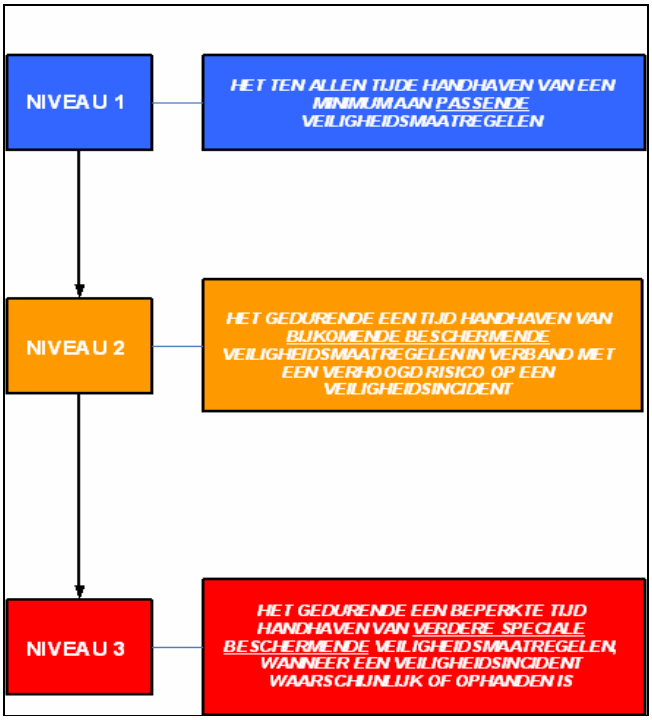
- Het opzetten van een internationaal raamwerk tussen regeringen en de scheepvaartindustrie
- Het nemen van preventieve maatregelen tegen veiligheidsincidenten
- Het vaststellen van taken en verantwoordelijkheden voor de bescherming van de maritieme veiligheid
- Het bezitten van een methode om de veiligheidssituatie te beoordelen
- Het beschikbaar hebben van plannen en procedures om te reageren op veiligheidsincidenten
- Het uitwisselen en verzamelen van beschikbare en gerelateerde informatie

De ISPS-code maakt een onderscheid tussen maatregelen die gelden voor schepen en maatregelen die van toepassing zijn op havenfaciliteiten die voor internationale reizen gebruikte schepen afhandelen (voorschrift 2). Deze maatregelen werken aanvullend en kunnen niet los van elkaar gezien worden.

De ISPS-code is van toepassing op de volgende soorten schepen die voor internationale reizen worden gebruikt:

- Passagiersschepen, met inbegrip van hogesnelheidspassagiersvaartuigen
- Vrachtschepen, met inbegrip van hogesnelheidsvaartuigen met een bruto tonnage van 500 of meer
- Booreenheden

De nationale overheden hebben een aantal verantwoordelijkheden op te nemen. Ze moeten de veiligheidsniveaus instellen en richtsnoeren verschaffen voor de bescherming tegen veiligheidsincidenten (A.4.1). Hogere veiligheidsniveaus verwijzen naar een hoger risico op een veiligheidsincident. De ISPS-code voorziet in drie ‘security levels’ (veiligheidsniveaus). Het eerste niveau is het basisniveau. Dit geldt altijd en betekent dat er steeds een handhaving is van een minimum aan beschermende veiligheidsmaatregelen. Het tweede niveau is het gedurende een bepaalde tijd handhaven van bijkomende beschermende veiligheidsmaatregelen, dit omwille van een verhoogd risico op een veiligheidsincident. Het derde niveau wordt ingesteld als er een veiligheidsincident waarschijnlijk of ophanden is. Wanneer dit niveau van kracht is worden er gedurende een beperkte tijd verdere speciale beschermende veiligheidsmaatregelen gehandhaafd. Elk veiligheidsniveau bestaat dus uit een uitbreiding van het voorgaande niveau. Deze veiligheidsniveaus kunnen samengevat worden in Figuur 1.



Figuur 1: Veiligheidsniveaus van de ISPS-code

Bron: Dominique Cant, P&O Ports, 14 mei 2004

Een havenfaciliteit of een schip is verplicht te reageren op de veiligheidsniveaus die worden ingesteld door de nationale overheid. In wat volgt worden enkel de verplichtingen besproken die van toepassing zijn op de havenfaciliteiten. Veiligheidsmaatregelen en –procedures dienen door de havenfaciliteit zodanig te worden toegepast dat eventuele verstoring of vertraging van passagiers, schepen, bemanning en bezoekers van schepen, goederen en diensten tot een minimum beperkt blijven (A.14.1). Wanneer veiligheidsniveau één van toepassing is, moeten de havenfaciliteiten de volgende activiteiten ondernemen (A.14.2):

- Zorg dragen voor de uitvoering van alle taken met betrekking tot de veiligheid van de havenfaciliteit
- De toegang tot de havenfaciliteit controleren
- Bewaking van de havenfaciliteit, met inbegrip van anker- en aanlegplaats(en)
- Bewaking van verboden terreinen, en zorgen dat alleen bevoegd personeel toegang heeft
- Toezicht op het laden en lossen van lading

- Toezicht op het laden en lossen van scheepsvoorraden
- Zorgen dat er veiligheidscommunicatiemiddelen binnen handbereik zijn

Hieruit blijkt dat het eerste veiligheidsniveau niet overeenkomt met de gewone bedrijfsvoering van een havenfaciliteit, zoals we die kenden vóór 1 juli 2004, het houdt veel meer in. Bij het tweede en het derde veiligheidsniveau worden deze maatregelen aangevuld met bijkomende beschermende maatregelen (A.14.3 en A.14.4).

2.2 Organisatie en verantwoordelijkheden

In de veertiende overweging van Verordening 725/2004 staat dat iedere lidstaat een centrale autoriteit moet aanwijzen die de toepassing van de veiligheidsmaatregelen in het zeevervoer op het nationale niveau coördineert en controleert. De lidstaten moeten zorgen voor de nodige middelen en voor een nationaal plan voor de implementatie van Verordening 725/2004. Bovendien dient er krachtens artikel 2.7 in elke lidstaat per zeehaven een 'Bevoegde Autoriteit voor Maritieme Beveiliging' aangewezen te worden. Hij of zij is verantwoordelijk voor de lokale tenuitvoerlegging en controle van de door Verordening 725/2004 voorgeschreven veiligheidsmaatregelen voor schepen en/of één of meer havenfaciliteiten.

In het vervolg van Verordening 725/2004 staan in verschillende artikelen de andere verantwoordelijkheden van de verdragsluitende staat vermeld. Deze zijn het uitvoeren van een veiligheidsbeoordeling (B.1.16 – dwingend), het instellen van de veiligheidsniveaus en het verschaffen van richtsnoeren voor de bescherming tegen veiligheidsincidenten (A.4.1), duidelijk aangeven en mededelen welke maatregelen moeten worden opgenomen per veiligheidsniveau in het veiligheidsplan en aangeven wanneer een veiligheidsverklaring moet worden opgesteld (voorschrift 10.3). De verdragsluitende staat moet volgens B.16.62 ook een 'Verklaring van naleving' afleveren.

2.3 Beveiliging van een havenfaciliteit

Een definitie van het woord havenfaciliteit is terug te vinden in de ISPS-code zelf. Een havenfaciliteit is een door de verdragsluitende regering of de aangewezen autoriteit vastgestelde locatie waar het schip/haven raakvlak plaatsvindt. Deze omvat onder meer ankerplaatsen, ligplaatsen en aanvaarroutes, naar gelang van toepassing. “Men spreekt over het raakvlak schip/haven wanneer er interacties plaatsvinden waarbij een schip rechtstreeks betrokken is bij de activiteiten waarbij sprake is van de verplaatsing van personen of goederen dan wel havendienstverlening aan het schip of vanuit het schip”. (Van Meel, 2005)

Het veiligheidsplan (verplicht volgens voorschrift 10.2.2) voor de havenfaciliteiten wordt opgesteld door de havenfaciliteitsveiligheidsbeambte (of port facility security officer, PFSO) op basis van een veiligheidsbeoordeling verricht door de verdragsluitende staat. Deze beoordeling mag ook worden uitgevoerd door een erkende veiligheidsorganisatie, maar enkel de nationale overheid heeft de bevoegdheid deze goed te keuren (A.4.3). Deze beoordeling bevat de volgende elementen (A.15.5 en B.15): evaluatie en identificatie van de goederen, gebouwen en infrastructuur, identificatie van mogelijke bedreigingen, beschrijving van de te nemen maatregelen en de identificatie van de zwakheden in de infrastructuur, beleid en procedures. Alle gebieden die relevant zijn voor de havenveiligheid en de havengrenzen moeten in overweging worden genomen tijdens de beoordeling. Afhankelijk van de boordeling kunnen er verschillende maatregelen, procedures of acties worden ingesteld per subgebied. (Van Meel, 2005)

Het veiligheidsplan dient bepalingen voor de drie veiligheidsniveaus te bevatten en volgens voorschrift 10.3 moeten de verdragsluitende staten duidelijk aangeven en mededelen welke maatregelen voor de verschillende niveaus moeten worden opgenomen. Het plan moet toereikend zijn voor het schip/haven raakvlak. Na de opstelling moet de verdragsluitende staat het veiligheidsplan goedkeuren. Het plan moet worden opgesteld in de werktaal of –talen van de havenfaciliteit. Het plan dient ten minste de volgende onderdelen te bevatten (A.16.3):

- Maatregelen om te voorkomen dat er voor gebruik tegen personen, schepen of havens bedoelde wapens of andere gevaarlijke stoffen en apparaten, waarvan het vervoer verboden is, de havenfaciliteit in of aan boord van een schip worden gebracht
- Maatregelen om te voorkomen dat onbevoegden toegang krijgen tot de havenfaciliteit, tot in de havenfaciliteit aangemeerde schepen, en tot de verboden terreinen van de havenfaciliteit
- Procedures waardoor kan gereageerd worden op veiligheidsbedreigingen of inbreuken op de veiligheid, met inbegrip van bepalingen betreffende de handhaving van kritische operaties van de havenfaciliteit of het schip/haven raakvlak
- Procedures waardoor kan gereageerd worden op eventuele veiligheidsinstructies die de verdragsluitende staat op wiens grondgebied de havenfaciliteit zich bevindt bij veiligheidsniveau 3 zou kunnen geven
- Procedures voor de evacuatie in geval van veiligheidsdreigingen of inbreuken op de veiligheid
- De taken voor de beveiliging van verantwoordelijk personeel van de havenfaciliteit en van ander personeel van de faciliteit in verband met beveiligingsaspecten
- Procedures voor de interfacing met de beveiligingsactiviteiten op het schip
- Procedures voor de periodieke beoordeling en bijwerking van het plan
- Procedures voor het melden van veiligheidsincidenten
- Identificatie van de veiligheidsbeambte van de havenfaciliteit, vergezeld van 24-uurs contactinformatie
- Maatregelen om de veiligheid van de in het plan vervatte informatie te waarborgen
- Maatregelen om een doeltreffende beveiliging van lading en laad- en losapparatuur binnen de havenfaciliteit te waarborgen
- Procedures voor het controleren van het veiligheidsplan van de havenfaciliteit
- Reactieprocedures wanneer het scheepsveiligheidsalarmsysteem in de havenfaciliteit is geactiveerd
- Procedures ter vergemakkelijking van walverlof voor het scheepspersoneel of personeelswisselingen en van de toegang van bezoekers tot het schip, waaronder afgevaardigden van welzijns- en vakbondsorganisaties voor zeelieden

Krachtens de artikelen B.16.58 en B.16.59 dienen er door de havenfaciliteit procedures te worden voorzien om de blijvende doeltreffendheid van het havenfaciliteitsveiligheidsplan te controleren, net zoals er procedures dienen te worden voorzien met betrekking tot de actualisering of wijziging van het veiligheidsplan. Dit naar aanleiding van veiligheidsincidenten waarbij de havenfaciliteit betrokken was of wijzigingen in het eigenaarschap of operationele beheer van de havenfaciliteit optraden.

Het is belangrijk om hier bij op te merken dat het veiligheidsplan van een havenfaciliteit een 'levend' document is. Het is niet iets dat opgesteld wordt om daarna nooit meer te bekijken. De havenfaciliteiten moeten er altijd voor zorgen dat het veiligheidsplan in overeenstemming is met de werkelijkheid.

Naast het verplichte veiligheidsplan kan er, mits er aan bepaalde voorwaarden wordt voldaan, ook een veiligheidsverklaring worden opgesteld. De verdragsluitende staten bepalen wanneer dit vereist is op basis van de risico's die het schip/haven raakvlak of de schip tot schip activiteiten opleveren voor personen, eigendommen of het milieu. Een schip kan een verzoek indienen om een veiligheidsverklaring op te stellen in de volgende gevallen (A.5.2):

- Wanneer het schip op een hoger veiligheidsniveau werkt dan de havenfaciliteit of het andere schip waarmee samenwerking plaatsvindt
- Wanneer er een overeenkomst betreffende een veiligheidsverklaring bestaat tussen verdragsluitende staten met betrekking tot bepaalde internationale reizen of specifiek daarvoor gebruikte schepen
- Wanneer er een veiligheidsbedreiging of veiligheidsincident is geweest, waarbij het schip of de havenfaciliteit betrokken was, naar gelang van toepassing
- Wanneer het schip zich in een haven bevindt die niet verplicht is over een goedgekeurd havenfaciliteitsveiligheidsplan te beschikken of uit te voeren
- Wanneer er schip tot schip activiteiten plaatsvinden met een ander schip dat niet verplicht is over een goedgekeurd scheepveiligheidsplan te beschikken of uit te voeren

Daarnaast kan ook een havenfaciliteit de opstelling noodzakelijk achten en hierom verzoeken. Gezien de toepassingsmodaliteiten van artikel 5.2 zal het opstellen van een

veiligheidsverklaring eerder uitzondering dan regel zijn. Bovendien kunnen de verzekeringstechnische gevolgen in geval van 'oneigenlijk of verkeerd gebruik van een veiligheidsverklaring' verregaande nefaste financiële gevolgen hebben voor een havenfaciliteit. De veiligheidsbeambte van de havenfaciliteit dient dus bijzonder voorzichtig met deze materie om te gaan.

Een model van een veiligheidsverklaring is opgenomen als aanhangsel van Verordening 725/2004. Het gaat hierbij om een model tussen een schip en een havenfaciliteit. Als er een veiligheidsverklaring moet worden opgesteld tussen twee schepen, moet het model worden aangepast.

Voor havenfaciliteiten met een zeer occasionele trafiek kunnen er in samenspraak met de nationale overheid alternatieve beveiligingsmaatregelen overeengekomen worden. Het gaat hier wel om uitzonderingen.

2.4 Veiligheidsbeambte van de havenfaciliteit

Het veiligheidsplan vermeldt dat elke havenfaciliteit een veiligheidsbeambte in dienst moet nemen en deze moet 24/24 en 7/7 bereikbaar zijn. Zijn taken en verantwoordelijkheden omvatten onder meer (A.17.2):

- De uitvoering van een eerste uitgebreid veiligheidsonderzoek van de havenfaciliteit, waarbij rekening wordt gehouden met de betreffende veiligheidsbeoordeling van de havenfaciliteit
- De zorg voor de ontwikkeling en het onderhoud van het havenfaciliteitsveiligheidsplan
- De uitvoering van het havenfaciliteitsveiligheidsplan en de daarmee verband houdende oefeningen
- De regelmatige uitvoering van veiligheidsinspecties in de havenfaciliteit om ervoor te zorgen dat passende veiligheidsmaatregelen gehandhaafd blijven

- Aanbevelingen doen voor wijzigingen van het havenfaciliteitsveiligheidsplan en deze daarin aanbrengen, naar gelang van toepassing, teneinde onvolkomenheden te corrigeren en het plan bij te werken in verband met van belang zijnde veranderingen in de havenfaciliteit
- De verhoging van de veiligheidsbewustheid en de waakzaamheid van het personeel van de havenfaciliteit
- Zorgen dat het personeel dat verantwoordelijk is voor de beveiliging van de havenfaciliteit voldoende getraind is
- De rapportage aan de betreffende autoriteiten en documentering van documentatie met betrekking tot voorvallen die bedreigend zijn voor de veiligheid van de havenfaciliteit
- De coördinatie van de uitvoering van het havenfaciliteitsveiligheidsplan met de betreffende veiligheidsbeambten van de maatschappij en de schepen
- De coördinatie met veiligheidsdiensten
- Zorgen dat wordt voldaan aan de normen die gelden voor personeel dat verantwoordelijk is voor de beveiliging van de havenfaciliteit
- Het waarborgen dat eventueel aanwezige veiligheidsapparatuur op de juiste wijze wordt gebruikt, getest, geijkt en onderhouden
- Scheepsveiligheidsbeambten, indien zij dit vragen, helpen bij de vaststelling van de identiteit van mensen die zij willen inschepen

2.5 Opleidingen en oefeningen

De IMO (International Maritime Organisation) voorziet in een aantal cursussen. In deze cursussen wordt dieper ingegaan op de verschillende aspecten van de ISPS-code. Men behandelt onder andere de toegang tot de havenfaciliteit, de ladingsbehandeling, de scheepsbevoorrading, enzovoort. Daarnaast gaat men dieper in op het algemene kader waarin de wetgeving kadert. Wat het beveiligen van de havenfaciliteit betreft, wordt er tijdens de cursussen dieper ingegaan op het begrip risico, risico-identificatie en inventarisatie, risico-evaluatie en beheersing. Men leert ook omgaan met ‘gevoelige informatie’ met betrekking tot de veiligheid en de communicatie over en rond de veiligheid. (Van Meel, 2005)

In deel B van de ISPS-code (B.18.6) wordt de aanbeveling gedaan om minstens éénmaal per kalenderjaar, met een periode van niet meer dan 18 maanden tussen de oefeningen, diverse soorten oefeningen uit te voeren. Hierbij kan er sprake zijn van deelname door de havenveiligheidsbeambten, samen met desbetreffende autoriteiten van de lidstaten, veiligheidsbeambten van schepen of van de maatschappij. Deze oefeningen moeten uitgevoerd worden met het oog op de veiligheid en implicaties voor de werkzaamheden van het schip. De communicatie, coördinatie, beschikbaarheid van hulpmiddelen en de reacties moeten worden getest. Deze oefeningen kunnen gebeuren op ware grootte, via computersimulaties of seminaries en gecombineerd worden met andere oefeningen zoals oefeningen op het gebied van reacties op noodsituaties.

Daarnaast vermeldt deel B van de ISPS-code (B.18.5) dat voor het waarborgen van de effectieve implementatie van de bepalingen in het veiligheidsplan van de havenfaciliteit er minstens elk kwartaal oefeningen moeten worden gehouden. Bij deze oefeningen moeten de verschillende onderdelen van het plan worden getest.

Hoofdstuk 3: De ISPS-code in België

3.1 Wetgeving in België

De IMO (International Maritime Organisation) heeft de ISPS-code uitgevaardigd. Deze is door de Europese Commissie overgenomen in Verordening 725/2004. Ter uitvoering van de internationale en Europese regelgeving werd in België op 15 juni 2004 een Koninklijk Besluit tot oprichting van een federaal comité en lokale comités voor de beveiliging van havenfaciliteiten opgesteld. In dit Koninklijk Besluit worden de verantwoordelijkheden aangeduid van het federaal comité, alsook de verantwoordelijkheden van de lokale comités. Verder wordt de samenstelling van deze comités behandeld.

Het Federaal Comité voor de Beveiliging van Havenfaciliteiten (FCBH) gaf op 25 mei 2004 de eerste praktische richtlijnen via de zogenaamde 'sjablonen'. Deze praktische richtlijnen zijn er gekomen om te voldoen aan voorschrift 10 van de Verordening. De enige toegevoegde waarde van deze 'sjablonen' is hun amusementswaarde, ze staan niet voor niets bekend als de 'Playmobil-sjablonen'. Daarbij komt dat de sjablonen niet conform met Verordening 725/2004 (A.14.2) zijn en dat sommige van deze 'sjablonen' in praktijk moeilijk toepasbaar zijn.

Het federaal comité heeft ten slotte ook nog aanbevelingen gedaan om te zorgen voor uniformiteit wat omheiningen en dergelijke betreft. Deze zijn er gekomen na overleg met de havenfaciliteiten zelf.

3.2 Organisatie en verantwoordelijkheden

In artikel 2 van het Koninklijk Besluit van 15 juni 2004 wordt de taak van het federaal comité als volgt omschreven: 'het federaal comité heeft tot taak om de federale, de Waalse en de Vlaamse regering, de Brusselse Hoofdstedelijke Gewestregering een algemeen beleid inzake de beveiliging van de havenfaciliteiten voor te stellen'. Verder wordt er vermeld dat het

federaal comité moet fungeren als een 'centrale nationale autoriteit' zoals voorzien in de ISPS-code. De taken van het federaal comité kunnen als volgt worden omschreven (artikel 2, Koninklijk Besluit 15 juni 2004):

- De algemene coördinatie van de beveiligingsmaatregelen tot implementatie van de nationale en internationale regelgeving met betrekking tot de beveiliging van havenfaciliteiten. Om deze coördinatie te kunnen uitvoeren wordt er een permanente commissie van experts opgericht. Deze commissie heeft als taak de beleidsadviezen van het federaal comité om te zetten in praktisch uitvoerbare richtlijnen voor de lokale comités. In de commissie zetelen experts vanuit verschillende disciplines. Het gaat hier zowel om nautische als veiligheidsexperts
- De adviesverlening aan de bevoegde overheden betreffende de wenselijkheid van de toepassing van bijkomende maatregelen die de beveiliging van de havenfaciliteiten verhogen
- De coördinatie van studies betreffende beveiligingsproblemen
- Het verstrekken van onderrichtingen en aanbevelingen aan de lokale comités
- Het fungeren als aanspreekpunt voor de verstrekking van inlichtingen over de beveiligingsplannen van havenfaciliteiten en als contactpunt voor maritieme beveiliging

Verder staat het federaal comité in voor de uiteindelijke goedkeuring van de veiligheidsbeoordelingen en veiligheidsplannen.

Het federaal comité[1] bestaat uit leden met stemrecht en leden zonder stemrecht en wordt voorgezeten door de directeur-generaal van het Directoraat-generaal Maritiem vervoer of zijn plaatsvervanger van de Federale Overheidsdienst (vanaf nu afgekort FOD) Mobiliteit en Vervoer. De leden met stemrecht zijn (artikel 3, Koninklijk Besluit 15 juni 2004):

- De directeur-generaal van het Algemene Directie Crisiscentrum of zijn vervanger van de FOD Binnenlandse Zaken

[1] Het federaal comité wordt voorgezeten door dhr. Frans Vanrompuy en is gevestigd op het volgende adres: Federaal Comité voor de beveiliging van de havenfaciliteiten, DG Maritiem Transport, Vooruitgangstraat 56, 1210 Brussel

- De administrateur-generaal van de Veiligheid van de Staat of zijn vervanger van de FOD Justitie
- De directeur-generaal van de administratie douane en accijnzen of zijn vervanger voor de FOD Financiën
- Een vertegenwoordiger van het Ministerie van Landsverdediging of zijn vervanger
- De directeur-generaal van het Directoraat-generaal Leefmilieu of zijn vervanger van de FOD Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu of zijn vervanger
- De directeur-generaal van de dienst Bilaterale Zaken van de FOD Buitenlandse Zaken of zijn vervanger

De leden zonder stemrecht zijn de vertegenwoordigers van de Gewesten en een vertegenwoordiger van elk lokaal veiligheidscomité.

Verder bepaalt het Koninklijk Besluit van 15 juni 2004 de oprichting van lokale beveiligingscomités in elke zeehaven (Antwerpen, Oostende, Zeebrugge en Gent) door het federaal comité. Het lokaal comité moet verantwoording afleggen van zijn werkzaamheden aan het federaal comité.

Het lokaal comité stelt een lijst op van de havenfaciliteiten die dienen te voldoen aan de ISPS-code. Tevens is het belast met de controle van de echtheid van de, door de havenfaciliteiten, geleverde inlichtingen en de beoordeling, op basis van een risicoanalyse, van de veiligheidsplannen. Vervolgens moet het deze gegevens ook opvolgen in de tijd.

De beveiligingsmaatregelen voor havenfaciliteiten gelegen buiten de zeehavengebieden langs rivieren en kanalen zullen gecoördineerd worden onder leiding van de directeur-generaal van de FOD Mobiliteitsafdeling voor maritiem vervoer in overleg met de waterwegbeheerders. Voor terminals langs rivieren en kanalen zal er een aparte regeling uitgewerkt worden op basis van ‘equivalent security arrangement’ of ESA. (Van Meel, 2005)

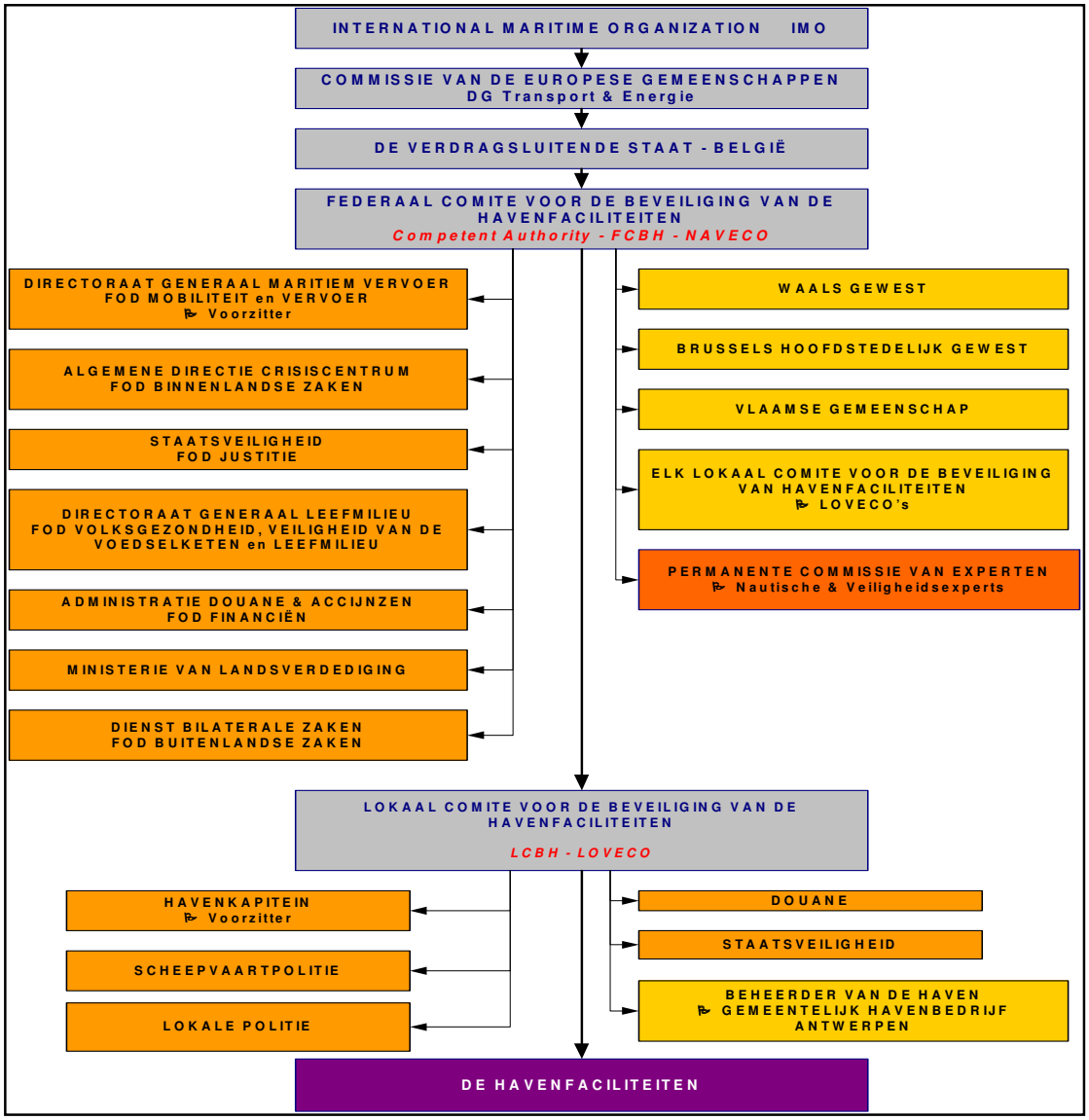
Het lokaal comité bestaat minstens uit de volgende leden:

- De havenkapitein of zijn vervanger
- De lokale politie
- De federale politie (scheepvaartpolitie)
- Douane
- Veiligheid van de Staat

Het lokaal comité[2] wordt voorgezeten door de havenkapitein. Als deze niet aanwezig is, wordt de voorzitter aangeduid door het federaal comité. De beheerder van de haven dient geen lid te worden van het lokaal comité, maar moet wel betrokken worden bij de werkzaamheden.
Het lokaal comité kan een beroep doen op de commissie van experts die behoren tot het federaal comité, maar het comité kan ook zelf experts toevoegen aan haar comité. Eventueel kan er een beroep gedaan worden op de expertise van de brandweer. (Van Meel, 2005)

[2] Het lokaal comité van de haven van Antwerpen kan bereikt worden op het volgende adres: Havenkapitein (commandant Jan Verbist), Entrepotkaai 1, 2000 Antwerpen, tel. 03/205.20.11 – Fax 03/205.22.70

Het bovenstaande kan samengevat worden in een Figuur 2.



Figuur 2: Overzicht van de bevoegde organisaties en hun leden

Bron: Dominique Cant, 22 juni 2004, P&O Ports

De verschillende kleuren op Figuur 2 geven de bevoegdheden weer. De oranje kleur duidt aan dat het gaat om leden met stemrecht, de gele kleur duidt de leden zonder stemrecht aan. De grijze kaders zijn de organisaties die verantwoordelijk zijn voor de tenuitvoerlegging en

coördinatie van de voorziene beveiligingsmaatregelen in de ISPS-code en in Verordening 725/2004.

Wat opvalt in deze figuur is dat het federaal en het lokaal comité beslissingen moeten nemen waarvan de gevolgen voor de havenfaciliteiten zijn. Maar deze worden nergens betrokken in het beslissingsproces. Dit is onlogisch, aangezien zij over de nodige expertise beschikken. Nu moeten zij maatregelen uitvoeren die misschien op een meer efficiënte manier hadden gekund. Aan de andere kant moet er rekening gehouden worden met de vertrouwelijkheid van sommige informatie afkomstig van de havenfaciliteiten. Als elke havenfaciliteit vertegenwoordigd zou zijn in het lokaal comité betekent dit ook dat ze de plannen van elkaar zouden moeten beoordelen. Dit kan leiden tot het vrijgeven van vertrouwelijke informatie van een bedrijf en dit kan dus de concurrentiepositie aantasten. Daarnaast is het onmogelijk om aan de eisen en verwachtingen van elke havenfaciliteit te voldoen, waardoor het beter is dat zij geen stemrecht hebben. Op die manier kunnen de leden met stemrecht de knoop doorhakken wanneer er beslissingen genomen moeten worden en er geen consensus wordt bereikt tussen de havenfaciliteiten. In de haven van Antwerpen worden de havenfaciliteiten wel betrokken bij de beslissingen, is er ruimte voor overleg, maar hebben ze inderdaad niet het laatste woord in de discussie. (Bron: Van Meel, persoonlijke communicatie)

3.3 Invoering van de ISPS-code in de haven van Antwerpen

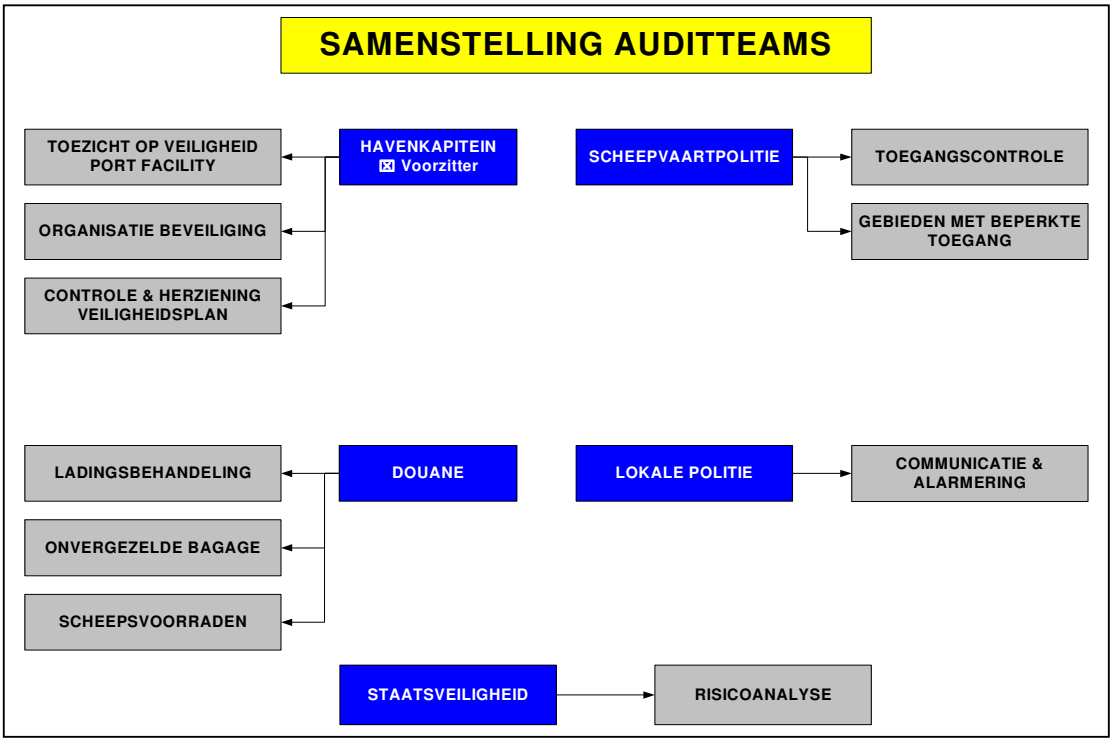
In dit deel wordt de invoering van de ISPS-code besproken zoals deze verlopen is in de haven van Antwerpen. Om de theorie te kunnen toetsen aan de praktijk wordt er een gevalstudie betrokken bij de bespreking, namelijk de havenfaciliteit P&O Ports.

Het implementatieproces van de ISPS-code bestaat uit verschillende stappen. De eerste stap die diende te gebeuren was het uitvoeren van een risicoanalyse van de havenfaciliteiten (PFSA, Port Facility Security Assessment). Volgens artikel B.1.16 moet deze beoordeling worden uitgevoerd door de verdragsluitende staat. Na de uitvoering van het PFSA, moet die goedgekeurd worden door de overheid. Nadien moet de veiligheidsbeamte van de

havenfaciliteit een risicoanalyse uitvoeren voor de havenfaciliteit waarvoor hij of zij verantwoordelijk is. Vervolgens wordt er overgegaan tot het opstellen van een veiligheidsplan voor de havenfaciliteit (PFSP, Port Facility Security Plan) en dat moet goedgekeurd worden door de aangewezen autoriteit. Vervolgens kan overgegaan worden tot de implementatie van het plan en deze implementatie wordt dan gecontroleerd door een erkende veiligheidsorganisatie (RSO, Recognised Security Organisation). Ten slotte wordt er een verklaring afgelegd dat de havenfaciliteit het plan naleeft. Deze verklaring kan gegeven worden door de aangewezen autoriteit of door de erkende veiligheidsorganisatie. Dit hele proces moest uitgevoerd zijn vóór 1 juli 2004.

In België heeft de overheid de verantwoordelijkheid voor de beoordeling van de havenfaciliteiten lang voor zich uitgeschoven en uiteindelijk hebben de havenfaciliteiten voorgesteld om deze beoordeling zelf uit te voeren. De vier havens van België hebben samen met de overheid dan beslist om de 'Port Facility Security Toolkit' aan te schaffen. De 'Toolkit' is een webgebaseerde applicatie die er voor moet zorgen dat de veiligheidsbeoordeling op een uniforme manier uitgevoerd wordt en dat zo de gerealiseerde plannen eveneens een uniforme vorm krijgen. De 'Toolkit' biedt de mogelijkheid om op een relatief eenvoudige manier een PFSA (Port Facility Security Assessment) uit te voeren. Dit PFSA is belangrijk voor het opstellen, controleren, evalueren en later wijzigen van het veiligheidsplan. De 'Toolkit' geeft de bedrijven via een overzichtelijke en gestructureerde vragenlijst inzicht in wat van hen verwacht wordt. Het maakt een complexe wetgeving toegankelijk. Na het beantwoorden van de vragenlijst levert het systeem automatisch een lijst af van de te ondernemen acties om aan de ISPS-vereisten te voldoen. Het geeft met andere woorden een stand van zaken. Daarnaast geeft het gegenereerde actieplan een overzicht van de kwetsbaarheden van de havenfaciliteit. De veiligheidsverantwoordelijke van de havenfaciliteit zal dan aan deze punten moeten werken. Als alle aandachtspunten zijn afgehandeld, kan men terugkeren naar de 'Toolkit'. Men vervolledigt dan de informatie met de uitgewerkte beveiligingsmaatregelen. Als er dan geen op- of aanmerkingen volgen, kan men een veiligheidsplan afdrukken dat alle beveiligingsmaatregelen bevat. Het veiligheidsplan kan dan beoordeeld worden door de bevoegde lokale autoriteiten. Eerst toetsen de auditteams, die binnen elk lokaal comité werden opgericht, het plan aan de

werkelijkheid waarna het ter goedkeuring wordt voorgelegd aan het federaal comité. Deze auditteams bestaan uit vijf groepen die elk een ander deel van het plan zullen controleren. Op Figuur 3 wordt de samenstelling van een auditteam weergegeven samen met de bevoegdheden van elk lid.



Figuur 3: Samenstelling van de auditteams

Bron: Dominique Cant, 22 juni 2004, P&O Ports

Er dient wel opgemerkt te worden dat het gebruik van de ‘Toolkit’ niet verplichtend is. Het PFSP kan ook op een andere manier tot stand gebracht worden. Een andere bemerking is dat de veiligheidsplannen die het resultaat zijn van deze ‘Toolkit’ niet conform zijn met de ISPS-regelgeving. Het is ook moeilijk om een risicoanalyse (een functionaliteit die door de ‘Toolkit’ ter beschikking wordt gesteld) uit te werken op computer die voor elk bedrijf correct is. Er zijn immers voor elke organisatie andere parameters nodig. Een beperkt aantal parameters zijn gelijk voor alle havenfaciliteiten, maar het overgrote deel is afhankelijk van het soort terminal, van het soort activiteiten, enzovoort.

P&O Ports heeft deze procedure ook doorlopen. Er werd een risicoanalyse uitgevoerd en nadien werd een veiligheidsplan opgesteld. P&O Ports heeft gewerkt met de 'Toolkit', maar zoals al eerder aangehaald vonden de mensen die instaan voor de beveiliging deze 'Toolkit' geen handig instrument. De risicoanalyse die uitgevoerd werd, was niet helemaal in overeenstemming met de noden van P&O Ports. Binnen het bedrijf is er dus nog een aanvulling geweest van de output van de 'Toolkit'. De havenfaciliteit is dus van mening dat de investering in de 'Toolkit' (ongeveer 250€ per havenfaciliteit) geen voordeel voor hen heeft opgeleverd. Na de opstelling van het veiligheidsplan moest dit gecontroleerd worden door het auditteam. Het auditteam heeft echter gecontroleerd op basis van plannen en niet op basis van de werkelijkheid. Hierdoor zijn er in België vergunningen uitgegeven aan havenfaciliteiten die op papier veel maatregelen treffen, maar in werkelijkheid niets doen ('formal compliance' tegenover 'physical compliance'). P&O Ports heeft er echter voor gekozen om zowel op papier als in de praktijk de voorschriften correct na te leven ('best in class-principe').

Andere praktijkervaringen van P&O Ports leren dat de inhoud van Verordening 725/2004 bij alle betrokken partijen te weinig gekend is. En dit fenomeen wordt alleen maar erger naarmate er meer beveiligingsinitiatieven bijkomen. Verder moeten de bewakingsagenten, die door een havenfaciliteit via een officieel erkende bewakingsfirma worden ingehuurd, een leerproces doorlopen. Er is dus bijgevolg een continue opvolging van de bewakingsagenten nodig. Een opmerking hierbij is dat in België slechts een aantal bedrijven bewakingstaken op zich mogen nemen, terwijl in Verordening 725/2004 staat vermeld dat de havenfaciliteiten deze taken ook zelf mogen uitvoeren als ze kunnen aantonen dat ze over de nodige deskundigheid beschikken. De kost van deze bewakingsagenten ligt heel hoog voor een havenfaciliteit en dus ook voor P&O Ports, terwijl ze het misschien zelf goedkoper en efficiënter zouden kunnen uitvoeren. Krachtens artikel B.16.8 (dwingend) heeft P&O Ports Key Performance Indicators (KPI's) geïntroduceerd om de doeltreffendheid van de bewakingsagenten continu te kunnen beoordelen. Een derde punt is dat de samenwerking met de NMBS vlot verloopt. Er zijn immers afspraken nodig geweest omdat volgens Verordening 725/2004 elke toegang tot de havenfaciliteit afgesloten moet zijn waaronder dus ook de toegang per spoor. Ten vierde: zoals al eerder werd aangehaald, wordt de expertise van de havenfaciliteiten niet gebruikt

binnen het federaal en het lokaal comité. In de praktijk is het wel zo dat het lokaal comité overleg pleegt met de havenfaciliteiten. Ten vijfde is er volgens P&O Ports ook dringend nood aan sensibilisering. Ten zesde verloopt de samenwerking met andere havenfaciliteiten meestal vlot, alsook de samenwerking met de buren. Een zevende praktijkervaring: P&O heeft er voor geopteerd om zijn perimeter te gaan beveiligen en niet elk onderdeel van de terminal. Dit om in overeenstemming te zijn met artikel A.14.1 van de Verordening. Dit artikel zegt dat veiligheidsmaatregelen en –procedures zodanig moeten worden toegepast dat eventuele verstoring of vertraging van passagiers, schepen, bemanning en bezoekers van schepen, goederen en diensten tot een minimum beperkt blijft. Indien P&O Ports elk afzonderlijk deel van zijn terminal zou afsluiten en beveiligen zouden er zich binnen de terminal wel vertragingen kunnen voordoen. Door de terminal als geheel af te sluiten en te beveiligen kan P&O Ports ook garanderen dat de terminal optimaal beveiligd is. Een achtste overweging is de veiligheidscontroles op goederen. Momenteel wordt er veel gecontroleerd, zoals de personen die toegang hebben tot een terminal, maar er zijn nog geen voorschriften over het controleren van goederen. Enkel de integriteit van de containerverzegeling (‘containerseal’) wordt gecontroleerd, maar dit was al een standaardprocedure vóór de invoering van de ISPS-code. Een negende punt is dat er ook geen duidelijke richtlijnen zijn voor het beveiligen van general cargo terminals. De door het federaal comité verschafte richtlijnen (de ‘sjablonen’) zijn absoluut ontoereikend en bovendien niet conform Verordening 725/2004. Een voorlaatste bemerking is dat P&O Ports vindt dat er gewerkt moet worden aan de communicatie, deze moet pro-actief en doelgericht worden. Ten laatste moet men rekening houden met het raakvlak ‘security-safety’ (beveiliging-veiligheid). Deze twee komen soms met elkaar in aanraking, bijvoorbeeld bij een evacuatie van de terminal. Zowel de verantwoordelijke van ‘Security’ als deze van ‘Safety’ dienen in voorkomend geval duidelijk te communiceren met elkaar zodat een eventuele evacuatie in optimale omstandigheden uitgevoerd kan worden. Bovendien wordt het opstellen van een evacuatieplan verplichtend gemaakt door de Verordening (A.16.3). Anderzijds kan een slecht ontworpen evacuatieplan tot heel hoge kosten leiden.

3.4 Veiligheidsbeambten in de haven van Antwerpen

Elke havenfaciliteit moet een veiligheidsbeambte aanstellen. De taken en verantwoordelijkheden van deze persoon werden besproken in het vorige hoofdstuk. Op de website van de haven van Antwerpen is een overzicht te vinden van de veiligheidsbeambten die actief zijn in de verschillende bedrijven die hun werkzaamheden hebben in de haven van Antwerpen. (http://www.portofantwerp.be/html/00_home/main_set_SO.html) (geraadpleegd op 5 april 2006)

Bij P&O Ports is Dominique Cant aangesteld als veiligheidsbeambte of PFSO (port facility security officer). Elke veiligheidsbeambte moet volgens artikel A.18.1 een opleiding hebben gekregen. Dominique Cant volgde zijn opleiding bij MUSC (Marine and Underwater Security Consultants). Deze organisatie biedt niet alleen opleidingen aan voor veiligheidsbeambten, maar ook diverse andere opleidingen. Daarnaast voert het bedrijf risicoanalyses uit voor havens, havenfaciliteiten en schepen en helpt het de organisatie bij het opstellen van veiligheidsplannen. Meer informatie hierover is te vinden op de website van MUSC (http://www.mandusc.com/index.cfm) (geraadpleegd op 5 april 2004)

De verantwoordelijke voor de veiligheid moet 7 dagen op 7 en 24 uur op 24 bereikbaar zijn. Hij moet beschikbaar zijn in het geval er zich een veiligheidsincident zou voordoen. Dit kan bijvoorbeeld voorkomen wanneer een persoon toegang probeert te krijgen tot een gebied van de terminal waarvoor hij niet bevoegd verklaard is.

3.5 Opleiding en trainingen

In België bieden een aantal organisaties cursussen aan in maritieme veiligheid. De ISPS-code legt namelijk de verplichting op om mensen op te leiden op het gebied van beveiliging. Dit werd al besproken in het voorgaande hoofdstuk. Het federaal comité kijkt na of de opleidingen van de organisaties wel conform de richtlijnen van de IMO zijn. Als dit het geval

is, krijgt de organisatie een erkenning van het federaal comité en mag het dus de opleidingen aanbieden.

Een eerste bedrijf dat deze opleidingen aanbiedt, is Group 4 Training nv. De opleidingen van dit bedrijf zijn in overeenstemming met de voorschriften van de IMO en de specifieke beveiligingswetgeving. Er is een opleiding tot PFSS (port facility security staff) en PFSO (port facility security officer). De opleiding tot PFSS is gericht aan het havenpersoneel. Het doel van de cursus is het havenpersoneel een aantal methodes en technieken bij te brengen zodat zij beter in staat zijn de beveiliging te garanderen. Zo leren zij bijvoorbeeld niet alleen een methodiek voor de beoordeling van de veiligheid van een havenfaciliteit, maar leren zij ook wapens, gevaarlijke stoffen en apparatuur te herkennen en op te sporen, en leren zij methodes voor inspectie, bewaking en toezicht, enzovoort. De opleiding tot PFSO is bedoeld voor de veiligheidsverantwoordelijken van zeehavens en havenfaciliteiten. Deze opleiding verloopt over drie dagen. De eerste dag leren de cursisten alles over de ISPS-code. De twee volgende dagen bekijkt men onder andere de overheidswetgeving, leert men omgaan met gevoelige informatie met betrekking tot de veiligheid en de communicatie over de veiligheid, bestudeert men methodes voor controle, inspectie, bewaking en toezicht en methoden voor oppervlakkige controle en het doorzoeken van bagage. De volledige inhoud van deze twee opleidingen kan geraadpleegd worden op de website van Group 4 (http://www.group4falck.be) (geraadpleegd op 5 april 2006). De tweede mogelijkheid is een cursus te volgen bij het BIHB (Beroepsinstituut voor Informatica, Haven en Beheer van goederenstromen). De belangrijkste taak van het BIHB is het trainen van werknemers van havenbedrijven. Recent is de doelgroep uitgebreid naar personen tewerkgesteld in de hele logistieke sector. Het instituut biedt een haven- en transportgerelateerde opleiding aan, zoals de opleiding tot PFSO. Daarnaast is er ook de mogelijkheid tot het volgen van taalcursussen en PC-cursussen. De lesgevers aan het BIHB zijn mensen met praktijkervaring, namelijk twee criminologen, één PFSO en één kapitein. Een derde mogelijkheid is een cursus te volgen bij de Hogere Zeevaartschool. Buiten deze organisaties zijn er natuurlijk nog andere bedrijven die dezelfde opleiding aanbieden.

Ook in het buitenland worden er door verschillende organisaties opleidingen voorzien. In het Verenigd Koninkrijk bijvoorbeeld worden deze gegeven door Marine and Underwater Security Consultants (MUSC) of het Renful Training Department.

Er moet wel opgemerkt worden dat niet alle opleidingen tegemoet komen aan de behoeften van de cursisten.

De contactgegevens van al deze bedrijven zijn terug te vinden in de bijlagen.

Hoofdstuk 4: Controle en handhaving

4.1 Inleiding

In dit hoofdstuk wordt nagegaan welke partijen zijn aangesteld om te controleren of de schepen en de havenfaciliteiten zich houden aan de verschillende maatregelen opgelegd door Verordening 725/2004. Verder wordt er weergegeven welke toepassingen er bestaan om de handhaving van de beveiligingsmaatregelen te garanderen. Ten slotte wordt aangegeven op welke manier P&O Ports probeert Verordening 725/2004 na te leven.

4.2 Wie controleert de naleving?

Er zijn inspecteurs aangesteld door de Europese Commissie die inspecties gaan uitvoeren in de landen die gebonden zijn door Verordening 725/2004 . Deze inspecties worden geregeld door Verordening 884/2005 van 10 juni 2005. Volgens de eerste overweging van deze Verordening dienen de inspecties te beginnen zes maanden na de inwerkingtreding van Verordening 725/2004. Op die manier kunnen de doeltreffendheid van de nationale systemen voor kwaliteitscontrole en de maatregelen, procedures en structuren voor de maritieme beveiliging gecontroleerd worden. Deze inspecties moeten uitgevoerd worden volgens een vaste procedure zodat de controles in alle lidstaten op dezelfde manier volbracht worden. In Verordening 884/2005 worden de procedures hiervoor vastgelegd, dit zowel op het niveau van de lidstaten, als op het niveau van de havenfaciliteiten en betrokken maatschappijen. Volgens artikel 5 van Verordening 884/2005 moeten de lidstaten nationale autoriteiten aanduiden die de inspecteurs van de Commissie kunnen bijstaan bij hun taken. In artikel 7 worden de kwalificatiecriteria en opleidingen aangehaald die de inspecteurs moeten bezitten om de controles te mogen uitvoeren. Zo moeten zij bijvoorbeeld een goed begrip hebben van maritieme beveiliging, een goede praktijkkennis van beveiligingstechnologieën en –technieken, enzovoort.

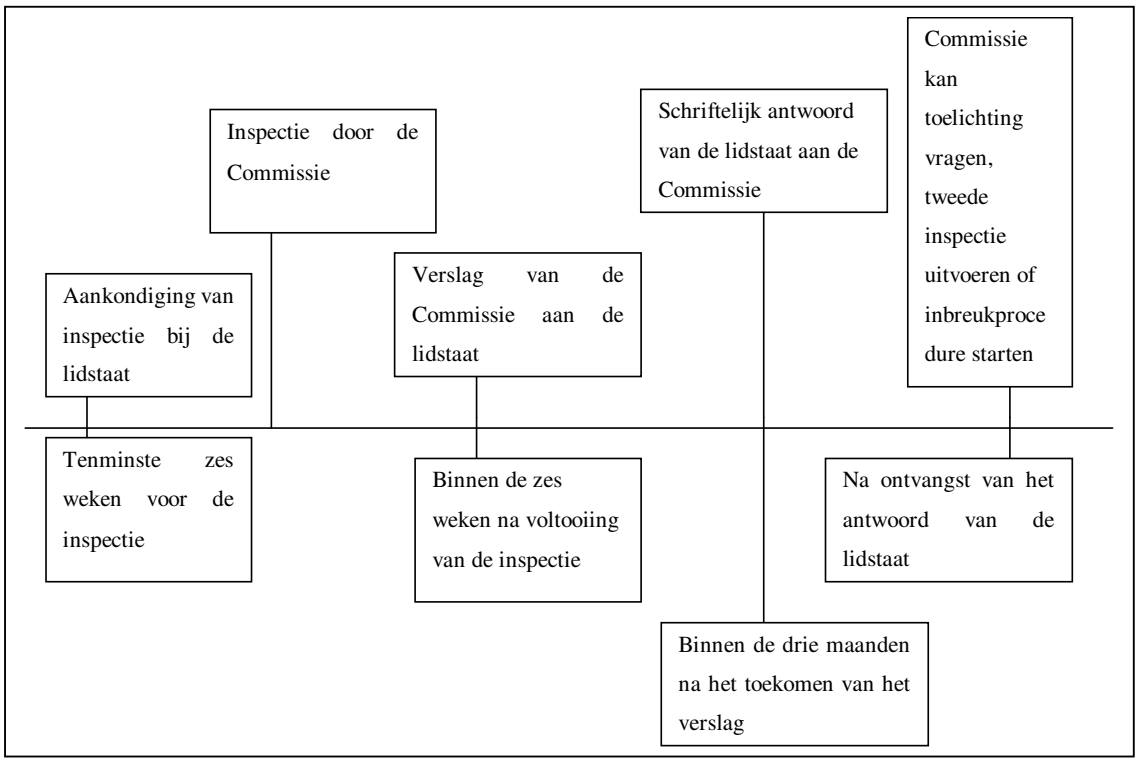
In hoofdstuk 2 van Verordening 884/2005 worden de procedures voor de uitvoering van inspecties van de Commissie uitgewerkt. De Commissie moet een inspectie tenminste zes weken op voorhand aankondigen bij de lidstaat. De lidstaat moet er voor zorgen dat de aankondiging van de inspectie vertrouwelijk blijft zodat het inspectieproces niet beïnvloed wordt. De inspecteurs moeten de nodige voorbereidingen treffen zodat de inspecties efficiënt en accuraat worden uitgevoerd. Binnen de zes weken na voltooiing van de inspectie stuurt de Commissie een verslag op naar de lidstaat. De lidstaat brengt dan de geïnspecteerde entiteiten op de hoogte van de relevante opmerkingen. In het verslag wordt gedetailleerd ingegaan op de opmerkingen gemaakt tijdens de inspectie, alsook elk (ernstig) gebrek aan overeenstemming met Verordening 725/2004 wordt gemeld. Het verslag kan ook aanbevelingen bevatten. De inspecteurs moeten aan elke opmerking in het verslag één van de volgende classificaties toepassen:

- In overeenstemming
- In overeenstemming, doch verbetering wenselijk
- Gebrek aan overeenstemming
- Ernstig gebrek aan overeenstemming
- Niet van toepassing
- Niet bevestigd

De lidstaten moeten dan binnen de drie maanden na het toekomen van het inspectieverslag een schriftelijk antwoord zenden aan de Commissie. In dit antwoord wordt ingegaan op de opmerkingen en aanbevelingen. Daarnaast moet er een actieplan voorgesteld worden met specifieke maatregelen en termijnen om de tekortkomingen weg te werken.

Na ontvangst van het antwoord van de lidstaat, kan de Commissie de lidstaat om een toelichting vragen om zo het geheel of delen van het antwoord te verduidelijken. Verder kan de Commissie een tweede inspectie uitvoeren om te controleren of de tekortkomingen worden weggewerkt. De Commissie kan ook een inbreukprocedure starten tegen de lidstaat.

Het bovenstaande kan samengevat worden op een tijdsschema en dit is terug te vinden op figuur 4.



Figuur 4: Tijdsschema van de inspecties

Bron: Eigen verwerking

In België is er een inspectie geweest in maart 2006 waarbij het federaal comité voor de beveiliging van havenfaciliteiten (FCBH) gecontroleerd werd. De inspecteurs hebben ook twee havenfaciliteiten gecontroleerd. Deze controles zijn enkel op papier uitgevoerd, dus de bedenking kan gemaakt worden of deze inspecties dan wel nuttig zijn.

Naast de controles van de Europese Commissie kan ook het federaal comité voor de beveiliging van havenfaciliteiten (FCBH) controles uitvoeren. Daarnaast kan het auditteam van een lokaal veiligheidscomité voor de beveiliging van havenfaciliteiten (LOVECO) naast de initiële controle van het veiligheidsplan nog bijkomende controles uitvoeren om na te gaan of de havenfaciliteiten zich houden aan de beveiligingsmaatregelen die ze zelf hebben vooropgesteld. Elke partij van het auditteam kan een controle uitvoeren binnen de toegewezen

bevoegdheden. De scheepvaartpolitie is verantwoordelijk voor de toegangscontrole en voor gebieden met beperkte toegang. De lokale politie kan controles uitvoeren op de communicatie en alarmering. De douane is bevoegd voor de ladingsbehandeling, de onvergezelde bagage en de scheepsvoorraden. De staatsveiligheid staat in voor de controles op de risicoanalyses. De havenkapitein ten slotte houdt toezicht op de veiligheid van de havenfaciliteiten, houdt zich bezig met de organisatie van de beveiliging en de controle en herziening van de veiligheidsplannen.

Naast deze partijen zijn ook ambtenaren van de FOD Mobiliteit en Vervoer en ambtenaren van de FOD Binnenlandse Zaken belast met het toezicht houden op de naleving van Verordening 725/2004. Dit wordt geregeld in een wetsvoorstel betreffende maritieme beveiliging dat het Koninklijk Besluit van 15 juni 2004 zal vervangen. De ambtenaren zijn eveneens bevoegd om de naleving van deze nieuwe wet te controleren. Ze mogen processen-verbaal opstellen om te bewijzen dat een havenfaciliteit zich niet houdt aan de bepalingen van Verordening 725/2004 en/of het wetsvoorstel betreffende maritieme beveiliging. Deze ambtenaren zullen dag en nacht, zonder voorafgaande verwittiging, plaatsen kunnen betreden waar Verordening 725/2004 en het wetsvoorstel van toepassing zijn. Verder zullen zij personen mogen verhoren en allerhande informatiedragers controleren. Om vaststellingen te kunnen doen, zullen zij ook bevoegd zijn om film- en video-opnamen te maken en foto's te nemen.

In artikel 14 van Verordening 725/2004 wordt aangehaald dat er sancties opgelegd dienen te worden indien er niet voldaan wordt aan de bepalingen van de Verordening. Er wordt ook vermeld dat deze sancties doeltreffend, evenredig en ontradend dienen te zijn. In het Koninklijk Besluit van 15 juni 2004 worden geen sancties bepaald. Maar in het wetsvoorstel betreffende maritieme beveiliging wordt dit onderwerp wel aangehaald. Er wordt een onderscheid gemaakt tussen administratieve en strafrechterlijke sancties. Als administratieve sanctie wordt aangehaald dat de nationale autoriteit voor maritieme beveiliging het verleende havenbeveiligingscertificaat kan intrekken indien een havenbeheerder of een havenfaciliteit niet heeft gehandeld volgens het havenbeveiligingsplan of het havenfaciliteitveiligheidsplan Verder kan het certificaat ook ingetrokken worden wanneer een havenbeheerder of een

havenfaciliteit heeft nagelaten te handelen volgens het havenbeveiligingsplan of het havenfaciliteitsveiligheidsplan. Er is ook sprake van administratieve geldboetes, maar dit is nog niet verder uitgewerkt in het wetsvoorstel. De strafrechterlijke sancties zijn als volgt omschreven in het wetsvoorstel betreffende maritieme beveiliging: "wordt gestraft met een gevangenisstraf van 6 maand tot 1 jaar en met een geldboete van 26 tot 3000 euro of met één van die straffen alleen, ieder die de bepalingen van Verordening 725/2004, alsook de bepalingen van de ter uitvoering van deze Verordening genomen besluiten, heeft overtreden." "Verder wordt gestraft met dezelfde straffen ieder die de opdracht van de bevoegde overheid uitgeoefend krachtens deze Verordening en haar uitvoeringsbesluiten heeft belemmerd. Daarnaast wordt gestraft met een gevangenisstraf van 6 maand tot 1 jaar en met een geldboete van 26 tot 3000 euro of met één van deze straffen alleen, ieder die de bepalingen van de wet betreffende maritieme beveiliging heeft overtreden. En ieder wordt gestraft die de opdracht van de bevoegde overheid uitgeoefend krachtens deze wet heeft belemmerd".

4.3 Handhaving van de beveiligingsmaatregelen via toegangscontrole

Eén van de belangrijkste onderdelen van de beveiliging is de toegangscontrole. Het basisprincipe hiervan kan gehaald worden uit Verordening 725/2004 en uit de sjablonen opgesteld door de Belgische overheid. Er zijn drie onderdelen belangrijk om te zorgen voor een effectieve toegangscontrole. Deze drie principes zijn:

- WIE – toegangsregistratie (A.14.2 en sjabloon 5)
- WAAR – toegangscontrole (A.16.3.5 en sjabloon 5)
- WAAROM – het bevoegd verklaren (A.16.3.2)

Sjabloon 5 ('gevoelige terminal-container, security level 1') zegt dat toezicht en registratie van in- en uitgaande personen, voertuigen en goederen moet gebeuren. Artikel A.14.2 vermeldt dat de toegang tot de havenfaciliteit moet gecontroleerd worden, dat er bewaking moet zijn van de havenfaciliteit (met inbegrip van de aanlegplaatsen) en dat er bewaking moet zijn van de verboden terreinen. Er moet tevens gezorgd worden dat enkel bevoegd personeel toegang heeft. Artikel A.16.3.2 haalt aan dat er maatregelen voorzien moeten worden om te

voorkomen dat onbevoegden toegang krijgen tot de havenfaciliteit, de in de havenfaciliteit aangemeerde schepen en verboden terreinen van de havenfaciliteit. Artikel A.16.3.5 zegt dat er procedures moeten voorzien worden voor de evacuatie. Een goed systeem voor toegangscontrole is dus ook een onmisbaar gegeven voor het verplichte evacuatieplan. Je moet immers weten welke personen zich waar bevinden om op een doeltreffende wijze te kunnen evacueren.

In de haven van Antwerpen wordt gewerkt met de Alfapass[3] omdat deze methode voldoet aan de voorwaarden van de ISPS-code op voorwaarde dat de drie principes gelijktijdig worden toegepast. Als dit niet gebeurt, wordt de Alfapass een karikatuur van zichzelf en is er in de haven van Antwerpen een geautomatiseerd toegangscontrolesysteem waarvan iedereen de sleutel heeft. De Alfapass vraagt een screening van elke persoon. Deze screening moet gebeuren door de overheid, maar er moet vastgesteld worden dat dit helaas uitblijft. In de praktijk betekent dit dat dus ook malafide figuren een Alfapass kunnen aanvragen en het is dan aan de havenfaciliteit om die personen bevoegd te verklaren of niet. Door het ontbreken van een screening door de overheid, wordt met andere woorden de havenfaciliteit zelf een bedreiging, aangezien de havenfaciliteit de toegangsrechten toekent aan de Alfapass.

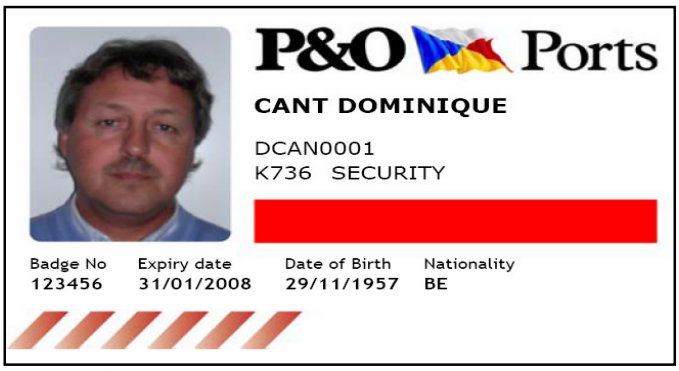
In de haven van Antwerpen wou men vermijden dat regelmatige bezoekers van de verschillende havenfaciliteiten voor elke maatschappij een ander toegangsbewijs zouden moeten voorleggen. Er wordt geschat dat er dagelijks ongeveer 20.000 à 30.000 mensen in de haven moeten zijn, namelijk 8.000 havenarbeiders, 10.000 à 15.000 vrachtwagenbestuurders, het personeel van de havenfaciliteiten en dan nog andere frequente bezoekers zoals onder andere kaai-expediteurs, scheepsagenten, waterklerken. Daarom bleek één overkoepelende ID-kaart de oplosssing. Er werd een studie uitgevoerd naar de haalbaarheid om een dergelijke kaart in te voeren in de haven van Antwerpen. Dit project kreeg de naam Alfapass - Port Access Security System. Begin 2004 werd er een vragenlijst naar de havenfaciliteiten gestuurd om na te gaan welke identiteitscontroles er op dat moment al uitgevoerd werden in de havenfaciliteiten. Op basis van deze antwoorden en andere conclusies van de studie, werden de krachtlijnen van de Alfapass uitgezet:

[3] Alfapass, Brouwersvliet 33/8, 2000 Antwerpen

- Een gemeenschappelijke ID-kaart voor de ganse haven
- Technologisch ondersteund
- De mogelijkheid om biometrische gegevens op te slaan
- Gekoppeld aan een centrale database

Omdat de ontwikkeling van een dergelijke kaart in het belang is van de hele havengemeenschap, hebben Alfaport Antwerpen en CEPA (vertegenwoordigers van de gemeenschap) samen met SEAGHA de vennootschap Alfapass opgericht. De organisatie zal instaan voor de basisinvestering, het uitgeven van de ID-kaarten en zal het kaartsysteem beheren en uitbaten. De kaart zelf wordt bekostigd door de havenfaciliteiten en zal drie jaar geldig zijn. Daarna moet de kaart vervangen worden, maar dit wordt gedekt door het abonnementsgeld dat de havenfaciliteiten betalen. Dit abonnementsgeld bedraagt 30 euro per jaar. Verder is er een éénmalige productiekost van 35 euro per kaart. Verder staan ze ook in voor het installeren van de leesapparatuur. De havenfaciliteiten bepalen zelf de toegangsrechten van de kaarthouders. Door de Alfapass te gebruiken weten de havenfaciliteiten altijd wie er zich op de terminal bevindt. Dit is nodig voor het vereiste evacuatieplan.

Op de Alfapass zijn de volgende gegevens van de kaarthouder zichtbaar: naam en voornaam, geboortedatum, nationaliteit, kaartnummer, geldigheidsdatum van de kaart, werkgever en een kleurenfoto. Op de chip van de kaart worden in elektronisch formaat de biometrische gegevens opgeslagen. Aan het unieke nummer van de kaart worden in de centrale database nog een aantal andere gegevens gekoppeld zoals het adres en het telefoonnummer van de kaarthouder. Op Figuur 5 is een voorbeeld te zien van een Alfapass die een vaste werknemer van P&O Ports ontvangt. Figuur 6 toont een Alfapass die wordt gegeven aan bezoekers.



Figuur 5: Voorbeeld van een Alfapass voor een vaste werknemer

Bron: Dominique Cant, 27 mei 2006, P&O Ports

Figuur 6: Voorbeeld van een Alfapass voor een bezoeker

Bron: Dominique Cant, 27 mei 2006, P&O Ports

4.4 Handhaving via oefeningen

Jaarlijks dienen de havenfaciliteiten oefeningen te houden om te controleren of het veiligheidsplan en/of het evacuatieplan werkt. Zonder deze oefeningen is het immers onmogelijk om een oordeel te vellen over de genomen maatregelen. Momenteel ontbreekt echter een goede communicatie met de overheid. De havenfaciliteiten vragen aan de overheid en het FCBH om hun expertise op het gebied van oefeningen tegen terreuraanslagen, maar op dit verzoek wordt niet geantwoord. Verder zijn de havenfaciliteiten vragende partij om samen met de overheid oefeningen te organiseren, maar de overheid is niet bereid om mee te werken.

Nochtans is het houden van oefeningen een verplichting volgens Verordening 725/2004. Zonder de steun van de overheid kan een havenfaciliteit geen grote oefeningen houden. Volgens voorschrift 10.3 van Verordening 725/2004 moeten de verdragsluitende staten duidelijk aangeven en mededelen welke maatregelen in het veiligheidsplan van een havenfaciliteit voor de verschillende veiligheidsniveaus moeten worden opgenomen. Het is met andere woorden de overheid zelf die de maatregelen oplegt en dus zou ook de overheid moeten testen of de maatregelen in de praktijk wel werken en effectief zijn. Op dit ogenblik zijn de havenfaciliteiten dus beperkt tot kleinere oefeningen om na te gaan of het veiligheidsplan en/of het evacuatieplan werkt. Een betere communicatie is dringend nodig, net zoals een controle op deze oefeningen. De loutere bevestiging dat het veilig is, is helaas niet voldoende. Er moet ook gecontroleerd worden of de maatregelen effectief zijn om zo bij een reële dreiging zeker te zijn van de maatregelen en op die manier schade en/of slachtoffers te voorkomen.

4.5 Praktijk

Bij P&O Ports wordt gebruik gemaakt van de eerder beschreven Alfapass. De havenfaciliteit bepaalt zelf per individu (per Alfapasshouder) welke personen toegang krijgen tot welke terminals en er wordt streng toegekeken op het naleven van deze toegangsrechten. Alfapasshouders van wie op een terminal van P&O Ports een misbruik van de Alfapass wordt vastgesteld, worden voor een onbepaalde periode de toegang tot alle P&O Ports terminals ontzegd. Een misbruik van een Alfapass wordt door P&O Ports ook altijd als een veiligheidsincident gemeld aan het lokaal comité voor de beveiliging van havenfaciliteiten (LOVECO) . Het LOVECO dient in principe aan een dergelijk veiligheidsincident het nodige gevolg te geven. Tot nu toe heeft P&O Ports 230 veiligheidsincidenten gemeld aan het LOVECO, maar er moet vastgesteld worden dat het LOVECO enkel antwoordt dat ze de melding goed ontvangen hebben.

P&O Ports stuurt ook dagelijks bewakingsagenten het terrein op om na te gaan of het beveiligingsmateriaal (zoals onder andere hekwerk, poorten en slagbomen) nog in goede staat

is, de zogenaamde patrouillerondes. Hierdoor kunnen onvolkomenheden tijdig vastgesteld en hersteld worden. Op die manier is er minder kans op een inbreuk.

De havenfaciliteit P&O Ports werkt ook met camera's om de ganse havenfaciliteit 24u op 24u en 7 dagen op 7 in de gaten te houden. Per terminal heeft P&O Ports gemiddeld een tiental vaste camera's staan die alle ingangen (weg-spoor-water) controleren. Verder heeft P&O Ports langs de waterkant en op lichtmasten ook 'speedomes' (krachtige camera's met een enorm zoombereik) geïnstalleerd waarmee onder alle weersomstandigheden geobserveerd en opgenomen kan worden. Deze beelden worden dagelijks door de ingehuurde bewakingsagenten nauwlettend bekeken. De bewakingsagenten volgen voor het bekijken van de beelden een vooraf bepaalde methodiek. Deze methodiek is nodig omdat een individu nooit 24 uur naar beelden kan kijken zonder de concentratie te verliezen. P&O Ports vindt dat beveiliging doeltreffend moet zijn en dat de dure camera's dan ook correct moeten gebruikt worden. Hierdoor hebben alle 55 bewakingsagenten van P&O Ports zeer specifieke instructies gekregen over wanneer en hoe ze de beelden van de camera's moeten bekijken. Bijvoorbeeld de beelden van camera SP1K312 (camera van spoorpoort 1 aan kaai 312) worden tussen 22u en 6u om het uur gedurende 10 minuten bekeken en de bewakingsagenten moeten dan controleren op beveiligingsinbreuken aan die spoorpoort. Enkel door deze gerichte observaties kan er aan doeltreffende beveiliging gedaan worden. Via deze methodiek kunnen inbreuken snel geconstateerd worden en kan er tijdig ingegrepen worden.

P&O Ports probeert zich zo veel mogelijk te houden aan de verplichting om oefeningen uit te voeren. Zij zijn vragende partij naar de overheid toe.

Er kan dus besloten worden dat de havenfaciliteit P&O Ports de nodige moeite doet om Verordening 725/2004 na te leven. De kans op een inbreuk wordt zo klein mogelijk gehouden. Het is echter zeer moeilijk om een doeltreffende ISPS-beveiliging te organiseren omdat er door het federaal comité voor de beveiliging van havenfaciliteiten (FCBH) buiten de 'sjablonen' nooit doeltreffende beveiligingsmaatregelen zijn gegeven zoals voorzien in voorschrift 10.3 van Verordening 725/2004.

Hoofdstuk 5: De kost van de beveiligingsmaatregelen

5.1 Inleiding

In dit hoofdstuk wordt eerst een studie besproken die gemaakt werd door het OECD (Organisation for Economic Co-operation and Development) over het totale kostenplaatje van de beveiligingsmaatregelen. Deze studie wordt gebruikt omdat de Europese Commissie nog geen eigen studie heeft uitgevoerd, hoewel dit vermeld staat in Verordening 725/2004. Daarna wordt de studie vergeleken met de praktijkervaring van P&O Ports. Ten slotte wordt de juridische kant van de beveiligingsmaatregelen bekeken.

5.2 Bevindingen OECD-studie[4]

In de OECD-studie wordt een onderscheid gemaakt tussen vijf categorieën. In de onderstaande bespreking zijn deze categorieën ondergebracht in drie onderverdelingen. Er wordt een onderscheid gemaakt tussen maatregelen die de overheid moet implementeren, maatregelen die van toepassing zijn op schepen en rederijen en maatregelen die van toepassing zijn op de havenfaciliteiten. Per categorie wordt nagegaan welke kosten er direct of indirect verbonden kunnen zijn aan de beveiligingsmaatregelen. Deze kosten zijn berekend in Amerikaanse dollars. De totale kosten zijn verrekend naar de euro met de koers van 18 april 2006 (EUR 1 = USD 1,225). In dit onderzoek wordt uitgegaan van 43.291 schepen (het aantal schepen ingeschreven in het Lloyd's Register in 2001).

5.2.1 Maatregelen die de overheden moeten implementeren

Zoals al eerder aangehaald zijn de overheden verantwoordelijk voor het instellen van de veiligheidsniveaus. In de OECD-studie wordt verwacht dat de kosten die gepaard gaan met het ontwikkelen van de veiligheidsniveaus klein zullen zijn. Daarentegen zullen de kosten die

[4] Security in maritime transport: Risk factors and economic impact, july 2003

gepaard gaan met de toepassing van de niveaus groot zijn en dan voornamelijk bij niveau 2 en 3. Bij het instellen van het tweede niveau wordt vooral een stijging verwacht van de arbeids- en tijdskosten (bijvoorbeeld om containers te scannen). Wanneer het derde niveau wordt ingesteld zullen er verstorende effecten optreden, zoals de evacuatie van een schip. Er zal dus vooral een stijging plaatsvinden van de indirecte kosten, de grootte hiervan is afhankelijk van de duur van het alarm. Naast deze kosten zal de overheid ook kosten hebben die gepaard gaan met een aantal andere verantwoordelijkheden zoals het uitvoeren van een risicoanalyse.

- ✓ Directe kosten: laag
- ✓ Indirecte kosten: mogelijk heel hoog

5.2.2 Maatregelen die van toepassing zijn op schepen en rederijen

In de ISPS-code zijn een aantal verplichtingen terug te vinden die schepen aanbelangen. Van drie van deze verplichtingen is een schatting gemaakt van de kosten. Het gaat om het automatische identificatiesysteem (AIS), het scheepsidentificatienummer en het scheepsalarmsysteem.

Het automatische identificatiesysteem is een communicatiemiddel aan boord van het schip dat in verbinding staat met andere zenders en op die manier basisinformatie over het schip doorgeeft. Elk schip moet hier mee uitgerust worden en de gemiddelde prijs voor een dergelijke zender ligt tussen de USD 10.000 en 20.000. De totale kost wordt geschat op USD 649,3 miljoen (USD 15.000 x 43.291 schepen). Deze kost mag niet gezien worden als een beveiligingskost opgelegd door de ISPS-code, aangezien het verplichtend maken van het AIS al bezig was voor de inwerkingtreding van de ISPS-code. Daarnaast verwacht men ook kosten voor het ontwikkelen van ontvangstfaciliteiten aan land. Deze kosten moeten gedragen worden door de overheden, maar op het moment van de studie was het niet mogelijk om een schatting te maken van deze kosten. Verder is het volgens de ISPS-code ook geen verplichting om dergelijke ontvangstfaciliteiten te bouwen.

- ✓ Directe kosten: USD 649,3 miljoen of EUR 530 miljoen
- ✓ Indirecte kosten: onbepaald

Elk schip moet zijn identificatienummer duidelijk en permanent vermelden. Deze kosten worden geschat op USD 5.000 per schip.

- ✓ Directe kosten: USD 21,6 miljoen of EUR 17,6 miljoen
- ✓ Indirecte kosten: geen

Als laatste moeten de schepen uitgerust worden met een alarm. Dit alarm wordt geactiveerd als er zich een veiligheidsincident voordoet en waarschuwt automatisch de bevoegde autoriteiten. De industrie verwacht een kost van USD 2.000 per alarm en verder een onderhoudskost van USD 100 per jaar.

- ✓ Directe kosten: USD 86,5 miljoen of EUR 70,6 miljoen
- ✓ Indirecte kosten: USD 4,3 miljoen of EUR 3,5 miljoen (jaarlijkse onderhoudskost)

Elk schip moet een veiligheidsbeamte voor het schip (SSO, Ship Security Officer) opleiden en in dienst nemen. Op het moment dat de studie gemaakt werd (juli 2003), bleek al dat de rederijen deze functie gingen invullen door extra verantwoordelijkheden te geven aan een in dienst zijnde werknemer.

- ✓ Directe kosten: USD 29 miljoen of EUR 23,7 miljoen per jaar

Deel A van de ISPS-code legt geen verplichtingen op voor bijkomende uitrusting aan boord van het schip, maar uit deel B blijkt dat er toch wel extra uitrusting nodig zal zijn om te voldoen aan alle verplichtingen van de code. Deze extra uitrusting verschilt naargelang het scheepstype en omdat het niet verplichtend is zullen ook niet alle schepen dezelfde inspanningen leveren. De Amerikaanse ‘Coast Guard’ heeft een overzicht gemaakt van de kosten per scheepstype voor het extra materiaal. Dit overzicht is terug te vinden in Tabel 1.

Tabel 1: Overzicht van de extra uitrusting met de bijhorende kost

Item	Initial investment			Annual maintenance	
	Number	Cost/item (USD)	Total cost (USD)	Cost/item (USD)	Total cost USD)
Tanker					
Hand-held metal detector	1	200	200	10	10
Hand-held Radio	5	200	1 000	10	50
Lock	10	300	3 000	15	150
Light	5	400	2 000	20	100
Auto-intrusion alarm	5	500	2 500	25	125
Freight Ship					
Hand-held metal detector	2	200	400	10	20
Hand-held Radio	5	200	1 000	10	50
Lock	10	300	3 000	15	150
Light	5	400	2 000	20	100
Auto-intrusion alarm	5	500	2 500	25	125
Portable vapour detector (for explosives)	1	8 000	8 000	400	400

Bron: OECD-studie, juli 2003

Op basis hiervan kan Tabel 2 worden opgesteld. In deze tabel wordt een overzicht gegeven per scheepstype van de investeringskost en de onderhoudskost en worden ook totalen berekend. Voor de niet-Amerikaanse schepen wordt uitgegaan van het volgende benodigde materiaal: 0 ‘hand-held metal detectors’, 3 ‘hand-held radios’, 5 ‘locks’, 5 ‘lights’, 2 ‘auto-intrusion alarms’ en 0 ‘portable vapour detectors’. ‘Hand-held metal detectors’ zijn detectietoestellen om metaal op te sporen, ‘portable vapour detectors’ zijn apparaten om ‘vieze’ geuren op te sporen en ‘auto-intrusion alarms’ (vrij vertaald ‘anti-binnendringsysteem) kunnen bestaan in verschillende vormen, zoals infrarood detectoren, bewegingsdetectoren, enzovoort. In de OECD-studie wordt niet beschreven hoe men aan deze cijfers gekomen is, maar waarschijnlijk zijn de onderzoekers aan de kapiteins van de schepen gaan vragen hoeveel stuks ze van elk item nodig zouden hebben.

Tabel 2: Investeringskost per scheepstype

	Initial Investment per Vessel (USD)	Annual Maintenance per Vessel (USD)	Number of vessels (2001)	Total Initial Investment (USD)	Total annual maintenance (USD)
American Trading Tankers	8 700	435	1 587	13 805 852	690 293
American Trading Freight vessels (non-container)	16 900	845	3 852	65 098 757	3 254 938
World Container Fleet	16 900	845	2 756	46 576 400	2 328 820
Non- American Trading Tankers	5 100	255	9 496	48 430 214	2 421 511
Non- American Trading Freight Vessels (non Container)	5 100	255	25 600	130 560 013	6 528 001
Total			43 291	304 471 236	15 223 562

Bron: OECD-studie, juli 2003

- ✓ Directe kosten: USD 304,4 miljoen of 248,5 miljoen EUR
- ✓ Jaarlijkse onderhoudskosten: USD 15,2 miljoen of 12,4 miljoen EUR

Ten slotte moeten er aan boord van het schip bewijzen worden bijgehouden van een aantal zaken zoals veranderingen in het veiligheidsniveau, periodieke herziening van het veiligheidsplan, enzovoort. Op het moment dat de studie werd gemaakt, was er geen ervaring met deze materie. Er werd uitgegaan van het feit dat er weinig tijd nodig is voor deze materie en dat dus de kosten ook laag zullen zijn.

- ✓ Directe kosten: laag

Verder legt de ISPS-code een aantal verplichtingen aan de rederijen op. Een eerste verplichting is de aanduiding van een CSO (Company Security Officer). Op het moment van de studie (juli 2003) namen grote rederijen een extra werknemer aan voor deze baan, maar kleinere rederijen gingen een bestaande werknemer deze taak op hem of haar laten nemen. De Amerikaanse 'Coast Guard' schat de kosten voor het in dienst nemen van een CSO voor een grote rederij op USD 150.000 per jaar en voor een kleine rederij op USD 37.500 per jaar. In deze studie werd een rederij als groot beschouwd vanaf tien schepen. Er wordt voor internationale grote rederijen ook een kost van USD 150.000 aangenomen. Volgens de Lloyd's List zijn er 12.987 rederijen over de hele wereld. In deze studie wordt verondersteld dat 50% (6.494) van deze rederijen actief zijn in de internationale handel. Er bestaan geen cijfers over het aantal rederijen dat meer dan tien schepen heeft. Daarom neemt men in deze

studie aan dat 50% (3.247) meer dan tien schepen bezit. De training van een CSO wordt geschat op USD 3.500 per jaar en het trainen van andere personeelsleden op USD 5.000 per jaar. Al deze gegevens samengenomen komen de kosten voor een grote rederij op ongeveer USD 514,6 miljoen per jaar. Voor kleine rederijen is de kost moeilijker te bepalen. Deze rederijen zijn werkzaam in lokale gebieden en daarvan zijn de gegevens zeldzaam. De rederijen schatten deze kosten op USD 100 tot USD 200 miljoen per jaar. In deze studie neemt men een gemiddelde.

- ✓ Directe kosten (grote bedrijven): USD 514,6 miljoen of EUR 420 miljoen per jaar
- ✓ Directe kosten (kleine bedrijven): USD 150 miljoen of EUR 122 miljoen per jaar

Een tweede verplichting is het uitvoeren van een SSA (Ship Security Assessment) of een risicoanalyse van het schip. De 'Coast Guard' schat dat er zestien uren nodig zijn voor het uitvoeren van zulk een analyse en dit aan USD 100 per uur. Volgens de rederijen zijn dit te weinig uren en schatten zij dat er drie tot vier dagen nodig zijn om een dergelijke analyse te maken. Daarom wordt in de studie aangenomen dat er drie dagen van acht uur nodig zijn om een SSA uit te voeren.

- ✓ Directe kosten: USD 103,9 miljoen of EUR 84,8 miljoen

De derde verplichting is het opstellen van een veiligheidsplan (SSP, Ship Security Plan). Er wordt aangenomen dat het opstellen van een SSP ongeveer twaalf uur in beslag neemt aan USD 100 per uur.

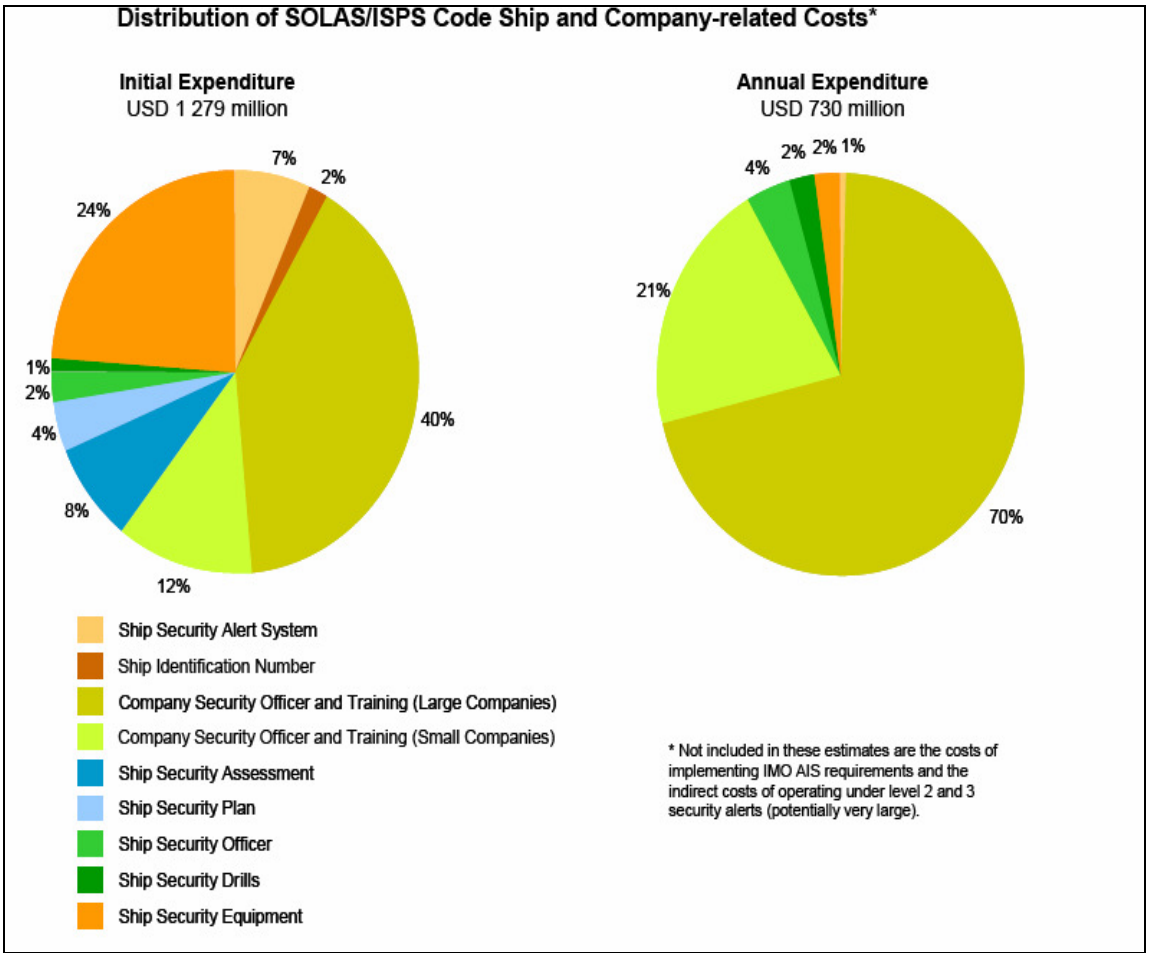
- ✓ Directe kosten: USD 51,9 miljoen of EUR 42,4 miljoen

Er moeten ook trainingen en oefeningen worden voorzien. In het onderzoek wordt uitgegaan van vier trainingen per jaar omdat in de ISPS-code de aanbeveling staat om elke drie maanden een oefening te houden. Er wordt aangenomen dat bij elke oefening vijftien mensen betrokken zijn, alsook de veiligheidsbeambte van het schip.

- ✓ Directe kosten: USD 16,8 miljoen of 13,7 EUR miljoen per jaar

Als we al deze maatregelen samen nemen dan is de initiële kost voor de rederijen minstens USD 1.279 miljoen of EUR 1.044 miljoen en daar komt een kost van USD 730 miljoen of

EUR 596 miljoen per jaar bij. Niet inbegrepen in deze schatting zijn de kosten van het installeren van een automatisch identificatiesysteem en de mogelijke indirecte kosten wanneer er gewerkt moet worden op veiligheidsniveau 2 of 3. Op Figuur 7 wordt een verdeling van deze totale kost gegeven over de verschillende verplichtingen.



Figuur 7: Verdeling van de totale kost over de verschillende verplichtingen

Bron: OECD-studie, juli 2003

5.2.3 Maatregelen die van toepassing zijn op de havenfaciliteiten

De ISPS-code legt een aantal verplichtingen op aan de havenfaciliteiten. Deze werden al uitgebreid besproken in de vorige hoofdstukken. Het bepalen van deze kosten is heel moeilijk aangezien er wereldwijd heel veel havens zijn en omwille van de verscheidenheid van deze havens. Het Departement van Transport van de Verenigde Staten identificeert minstens 3.970 havens over de hele wereld. Het Lloyd's Register telt er 2.814. In deze studie wordt gebruik gemaakt van het laatste cijfer. Verder gaat men uit van 6.500 havenfaciliteiten over de hele wereld.

Een eerste verplichting die opgelegd wordt is het uitvoeren van een PFSA (Port Facility Security Assessment). Deze kost zal verschillen per havenfaciliteit, afhankelijk van de grootte en van het feit of de havenfaciliteiten meer doen dan de minimumvereisten van de ISPS-code. De Amerikaanse 'Coast Guard' schat de kosten voor het uitvoeren van een risicoanalyse op USD 8.000 initieel en op USD 400 jaarlijks. Voor kleinere havenfaciliteiten worden de kosten geschat op USD 4.000 initieel en USD 100 jaarlijks.

- ✓ Directe kosten: USD 27,9 miljoen of EUR 22,8 miljoen
- ✓ Jaarlijkse onderhoudskosten: USD 0,8 miljoen of EUR 0,65 miljoen

Vervolgens moet er een veiligheidsplan (PFSP) opgesteld worden. Ook deze kosten variëren met de grootte van de havenfaciliteit, met de operaties die verricht worden, enzovoort.

- ✓ Directe kosten: USD 27,9 miljoen of EUR 22,8 miljoen
- ✓ Jaarlijkse onderhoudskosten: USD 0,8 miljoen of EUR 0,65 miljoen

Daarnaast moet er ook een veiligheidsbeambte aangeduid worden. De kosten bepalen van deze mensen is heel moeilijk omwille van diverse redenen. Ten eerste omdat een veiligheidsbeambte kan instaan voor meerdere havenfaciliteiten. Ten tweede omdat er geen gegevens bekend zijn over de internationaal geldende lonen in de verschillende havens.

Ten slotte moeten er ook trainingen gehouden worden en moet er geïnvesteerd worden in extra uitrusting. De kosten hiervan zijn moeilijk te bepalen door de grote variabiliteit in de

kosten tussen de verschillende havens. De uurlonen verschillen per land, de kost van materiaal is ook afhankelijk van lokale constructies en uurlonen, sommige havens en havenfaciliteiten hebben al meer gedaan aan veiligheid en beveiliging dan andere, enzovoort.

Om toch een idee te geven van al deze kosten is in de OECD-studie een schatting opgenomen voor de Amerikaanse havenfaciliteiten. Deze is terug te vinden in Tabel 3.

Tabel 3: Schatting van de kosten voor de Amerikaanse havenfaciliteiten

American Initial and Annual ISPS Code Compliance Costs by Category (million USD)				
Category	Initial Cost	*Percent of Total*	Annual Cost	*Percent of Total*
Port Facility Security Assessment	23	*2*	1	*0*
Port Facility Security Plan	23	*2*	1	*0*
Port Facility Security Officer	335	*35*	335	*63*
Security Training	17	*2*	17	*3*
Port facility Security Drills	0	*0*	35	*7*
Security Guards	124	*13*	124	*23*
Security Equipment	441	*46*	22	*4*
Total	**963**	*100*	**509**	*100*

Bron: OECD-studie, juli 2003

Uit Tabel 3 kan afgeleid worden dat het totale kostenplaatje gedomineerd wordt door de kost voor de PFSO en de bewakingsagenten. Er moet opgemerkt worden dat de bovenstaande cijfers niet zo maar kunnen overgenomen worden voor andere landen, aangezien de arbeidskosten internationaal sterk verschillen.

Vervolgens worden in de OECD-studie de kosten besproken die verbonden zijn met andere beveiligingsinitiatieven zoals C-TPAT en CSI. Voor meer informatie hierover wordt verwezen naar de OECD-studie. Voor meer informatie over deze andere beveiligingsinitiatieven wordt verwezen naar hoofdstuk 6.

5.3 Bespreking van de studie vanuit de praktijkervaring van P&O Ports

De inhoud van de OECD-studie komt niet overeen met de praktijkervaring van P&O Ports. In dit deel wordt geprobeerd aan te geven waar de studie niet overeenkomt met de praktijk en/of waar er aanpassingen in de OECD-studie nodig zijn.

In de OECD-studie wordt er gesproken over de maatregelen die de overheden moeten implementeren en wordt er gezegd dat de indirecte kosten hiervan hoog kunnen oplopen. Als er gekeken wordt naar de werkelijkheid dan is de grootste kost voor de overheid een administratieve kost. Dit houdt de kost in van het opvolgen en bijhouden van allerlei gegevens zoals de verschillende veiligheidsniveaus die van kracht geweest zijn. In de OECD-studie wordt aangehaald dat er geen kosten zijn voor het ontwikkelen van de veiligheidsniveaus, maar bijvoorbeeld op veiligheidsniveau 1 moeten er risicoanalyses worden uitgevoerd. Dus alvorens het eerste veiligheidsniveau kan ingesteld worden, zullen er al een aantal kosten gemaakt zijn. Wanneer er overgegaan wordt naar het tweede of derde veiligheidsniveau, veronderstelt de studie hoge kosten voor de overheid, maar in werkelijkheid heeft de overheid slechts minimale kosten wanneer dit voorvalt. De overheid moet enkel aan de havenfaciliteiten laten weten dat er een verhoging of verlaging van het veiligheidsniveau is. Het zijn dus de havenfaciliteiten die extra maatregelen zullen moeten nemen en bijgevolg ook de hoge kosten zullen dragen. Ten slotte vermeldt de OECD-studie dat er zowel verstorende effecten kunnen optreden bij het instellen van het derde veiligheidsniveau, als ook competitievervalsende effecten, bijvoorbeeld omdat het federaal comité voor de beveiliging van de havenfaciliteiten nooit aangegeven heeft welke beveiligingsmaatregelen er geïmplementeerd dienen te worden zal elke havenfaciliteit naar eigen goeddunken artikel B.16.3 in de praktijk omzetten. Dit artikel geeft weer dat elk havenfaciliteitsveiligheidsplan onder andere de operationele en fysieke maatregelen moet beschrijven die worden getroffen bij veiligheidsniveau 1. Verder moet elk veiligheidsplan de extra maatregelen beschrijven die van toepassing zijn bij veiligheidsniveau 2 en 3. Als een havenfaciliteit in zijn veiligheidsplan te weinig aandacht heeft hiervoor kan het door zijn verzekeraars aansprakelijk gesteld worden omdat de havenfaciliteit dan verzaakt heeft om tegemoet te komen aan de dwingende richtlijnen van Verordening 725/2004. Op moment dat

er daadwerkelijk geëvacueerd moet worden, kan het voorgaande leiden tot concurrentieverstoring.

In de OECD-studie wordt aangehaald dat grote rederijen een extra werknemer in dienst zullen nemen, maar in de praktijk blijkt dat de taak van CSO meestal wordt toegewezen aan een bestaand personeelslid. Hierdoor zullen de kosten van deze verplichting ook lager liggen dan verondersteld in de OECD-studie. Een bestaande werknemer zal misschien iets meer loon krijgen, maar de kost is dan enkel die loonsverhoging. Het vorige loon moest al betaald worden, dus dit kan niet beschouwd worden als een kost in verband met beveiliging. Hetzelfde geldt voor het in dienst nemen van een SSO. Zoals in de OECD-studie wordt aangehaald, zal deze taak toegewezen worden aan een bestaande werknemer. Hierdoor kunnen deze kosten ook niet beschouwd worden als kosten veroorzaakt door de ISPS-code.

Verder kan het opstellen van het veiligheidsplan ook niet beschouwd worden als een echte kost omdat het in ieder geval deel uitmaakt van de vele dagdagelijkse administratieve taken van de CSO, de SSO of de PFSO.

Volgens de ISPS-code moet elk schip uitgerust worden met een scheepsidentificatienummer. Dit moet aangebracht worden op de romp van het schip en duidelijk zichtbaar zijn. Dit gebeurt door met verf het identificatienummer aan te brengen op het schip. In de OECD-studie schat men de kost hiervoor op USD 5.000 of EUR 4.081. Een kritische bedenking hierbij is welke verf er gebruikt wordt om te komen tot een dergelijk hoge kost. En verder hoe lang het duurt om het scheepsidentificatienummer aan te brengen om de loonkost zo hoog te krijgen.

In de OECD-studie wordt de bouw van ontvangstfaciliteiten aangehaald en vermeld dat deze niet verplicht gesteld worden door de ISPS-code. In de praktijk is dan ook te merken dat er weinig van dergelijke ontvangstfaciliteiten zijn gebouwd.

In Tabel 3 worden de kostencategorieën aangehaald die gedragen worden door de havenfaciliteiten. Deze tabel is echter te algemeen en bijgevolg ook onvolledig. De kosten waar P&O Ports mee geconfronteerd wordt, zijn hieronder terug te vinden:

- Personeel voor beveiliging (PFSO en medewerkers)
- Meetings en conferenties over beveiliging
- PFSA en audits (toolkit)
- PFSP, procedures en risicoanalyses
- Trainingen en opleidingen in verband met beveiliging
- Administratie in verband met beveiliging en rapporteren aan de autoriteiten
- ISPS-training voor het personeel
- IT-beveiliging (bijvoorbeeld antivirus software)
- Re-siting of backup-tapes units
- IT-hardware (inclusief software licenties en printers)
- Verzekeringspremie
- Project management voor de volledige integratie van het beveiligingssysteem
- Beveiligingsdiensten (24/24 - 7/7)
- Beveiligingsafdeling (inclusief kleding, opbergkasten, enzovoort)
- Hekken (automatisch)
- Slagbomen (automatisch)
- Omheining (zowel nieuwe als het verbeteren van de bestaande)
- Tourniquets (automatisch)
- Systeem om indringing binnen de perimeter te detecteren
- Bewakingsuitrusting
- CCTV (Closed Circuit Television)
- Intercom
- Bescherming van de voornaamste installaties en infrastructuur
- Bescherming van de nutsvoorzieningen (gas, water en elektriciteit)
- Radio- en telecommunicatiesystemen (fax, telefoon en gsm)
- Informatieborden en pictogrammen
- Beveiligingsmaatregelen voor nabijgelegen plaatsen

- Toegangscontrole (Pass systeem) met bijhorende database management (inclusief additionele hardware)
- Visual Gate System – OCR (Optical Character Recognition)
- Verlichting
- Onderhoud en reparaties van hekken, slagbomen, tourniquets, enzovoort
- Verhoging van de veiligheidsniveaus (evacuatie, vertraging van vrachtwagens, tijdsoponthoud, enzovoort)
- Voertuigen (voertuigen voor patrouilles, voertuig voor PFSO, enzovoort)
- Beschermende kledij voor bewakingsagenten
- Installatie, verhogen van het vermogen, glasvezelnetwerk
- Zoekuitrusting (zaklampen, spiegels voor onder een voertuig te controleren, detectors van explosieven, enzovoort)
- Reserve generator voor administratiegebouw
- Aanpassingen aan gebouwen
- Financiële kosten

Er dient opgemerkt te worden dat de kosten voor het beveiligingsmateriaal eerder een éénmalige investering zijn. Maar omwille van wijzigende omstandigheden kan het gebeuren dat er opnieuw moet geïnvesteerd worden, bijvoorbeeld wanneer de nationale overheid de nodige bijsturingen doet, wanneer er een aanslag gepleegd wordt op een havenfaciliteit waardoor er internationaal bijgestuurd wordt, enzovoort. De kosten voor de bewaking zijn wederkerende kosten, aangezien deze bewaking altijd nodig is. Er dient ook rekening te worden gehouden met steeds wederkerende onderhouds- en reparatiekosten die hoog kunnen oplopen aangezien er in veel beveiligingshardware hoogtechnologische toepassingen zijn verwerkt. Het feit dat veel beveiligingshardware ook computergestuurd is, maakt het totale kostenplaatje voor herstelling en onderhoud aanzienlijk duurder.

Als laatste moet gewezen worden op het gevaar van automatisering. In de praktijk wordt al te vaak waargenomen dat havenfaciliteiten opteren voor de beveiliging te automatiseren, maar zich zelden de vraag stellen of dat wel de optimale oplossing is. Een voorbeeld hiervan is het

plaatsen van honderden camera's en de beelden daarvan te laten bekijken door bewakingsagenten. Deze baan kunnen mensen geen acht uur geconcentreerd volhouden, waardoor de kans op veiligheidsincidenten reëel blijft. P&O Ports heeft ervoor gekozen om hun mensen dagelijks het terrein op te sturen en ze te laten controleren of alles goed verloopt, dit natuurlijk in combinatie met een aantal camera's, want men kan niet op alle plaatsen tegelijkertijd zijn. Het is belangrijk om voor de implementatie van een maatregel de vraag te stellen of het wel echt nodig is. Op die manier vermijden de havenfaciliteiten dat ze onnodig geld gaan uitgeven en hierdoor de beveiligingskosten de hoogte in jagen.

5.4 Juridisch[5]

5.4.1 Inleiding

In de aanhef van de Verordening 725/2004 wordt vermeld dat de toepassing van alle maatregelen van de ISPS-code belangrijke vragen oproept in verband met de financiering ervan. De financiering van een aantal extra beveiligingsmaatregelen mag geen concurrentieverstoring in de hand werken. Verder wordt in deze overweging een studie aangevraagd om te onderzoeken wat de mogelijkheden zijn om een Europees rechtskader op te zetten. Verder moet in deze studie nagegaan worden wat de reële kosten zijn van al de beveiligingsmaatregelen. Een degelijk rechtskader zou concurrentieverstoring moeten vermijden. De verstoring van de concurrentie kan bijvoorbeeld ontstaan uit een verschillende graad van overheidsfinanciering in de lidstaten. De Europese Commissie pleit voor duidelijke richtsnoeren over de kostenverdeling tussen publieke autoriteiten, havenbesturen en operatoren.

Om de financiering van een beveiligingsmaatregel te beoordelen is het onder andere belangrijk het onderscheid aan te geven of de betrokken maatregel wordt getroffen vanuit openbaar gezag of binnen het raam van een individuele dienstverlening aan een waterweg- of

[5] Deze paragraaf is gebaseerd op 'Juridische aspecten van de financiering van havenbeveiliging' van E. Van Hooydonk in Beveiliging in het vrachtvervoer

havengebruiker. Artikel 2.5 van de Verordening 725/2004 zegt: ‘de combinatie van preventieve maatregelen en personele en materiële middelen die het zeevervoer en de havenfaciliteiten moeten beschermen tegen dreigingen van opzettelijke ongeoorloofde acties’. Deze definitie brengt geen duidelijkheid, maar bevestigt dat de bescherming van het vervoer en de havens de doelstelling is. Er wordt echter niet gesteld of de nodige instrumenten hiervoor aangeduid moeten worden vanuit het openbaar gezag of moeten ingesteld worden door individuele dienstverleners.

Als een investering in beveiliging de openbare beveiliging dient, dan is een vorm van openbare financiering te verkiezen boven een doorrekening aan de gebruiker van bijvoorbeeld de haven. Voorbeelden van acties met een hoofdzakelijk openbaar karakter zijn de opstelling van veiligheidsplannen voor het ganse havengebied, het uitvoeren van algemene veiligheidscontroles, enzovoort. Op het eerste zicht lijkt het dus verantwoord dat deze kosten gedragen worden door de nationale overheid of door het waterweg- of havenbestuur en dat ze niet aan de gebruikers van de waterweg of de haven doorgerekend worden.

Wanneer echter een terminalexploitant een beveiligingsmaatregel doorvoert, kan die investering gezien worden als een dienstverlening aan de gebruikers van die terminal. Verder is het zo dat de meeste van de ISPS-voorschriften een aanscherping inhouden van al eerder doorgevoerde beveiligingsmaatregelen. Een hoger beveiligingsniveau zal leiden tot een verhoogde commerciële aantrekkelijkheid en lagere verzekeringspremies door vermindering van de risico’s. Hierdoor is het logisch dat deze kosten door de terminals zelf gedragen worden. Er dient opgemerkt te worden dat de verzekeringspremies gestegen zijn, ondanks het verlaagde risico.

Met het bovenstaande onderscheid zijn echter niet alle problemen opgelost. Voor verschillende beveiligingsmaatregelen is het moeilijk uit te maken of een maatregel voor de openbare veiligheid of enkel voor de gebruikers van een bepaalde terminal geldt. Is de uitvoering van veiligheidscontroles door overheidsambtenaren bij de in- en ontscheping van passagiers in een haven waar maar één passagiersdienst opereert goed voor de openbare veiligheid? Of is het een dienstverlening van de overheid aan een commerciële operator?

Uiteindelijk blijkt dus dat de vraag wie welke beveiligingsmaatregelen moet betalen een beleidsvraag is. Daarbovenop wordt door de verscheidenheid aan concrete situaties de uitwerking van een sluitend regelgevend raamwerk voor de financiering van havenbeveiliging niet eenvoudig.

5.4.2 Overheidssteun voor havenbeveiliging

In de Verenigde Staten ondersteunt de federale overheid de havens financieel bij het treffen van de nodige beveiligingsmaatregelen. Dit is mogelijk volgens section 70107 van de US Maritime Tranportation Security Act (2002). Tot dusver hebben de Amerikaanse havens al USD 708 miljoen ontvangen en heeft de AAPA (American Association of Port Authorities) er voor gezorgd dat er jaarlijks een budget voorzien wordt van USD 400 miljoen.

In Europa daarentegen zijn de centrale overheden minder bereid tot het verlenen van financiële steun. In Nederland verleende de overheid een beperkte financiële steun van EUR 118.000. Hiermee heeft de Rotterdamse haven de 'Toolkit' ter beschikking kunnen stellen aan de andere havens. De Belgische havens ontvangen geen steun van de Belgische of Vlaamse overheid. In het algemeen staan de Europese overheden weigerachtig tegenover steunverlening aan beveiligingsmaatregelen, maar hierin schuilt een risico voor concurrentievervalsing. Sommige betrokkenen pleiten dan ook voor het alleen toestaan van overheidssubsidies die uniform worden toegepast in heel Europa. Door het ontbreken van een regelgevend raamwerk kan deze uniformiteit niet worden gegarandeerd.

Het treffen van bepaalde beveiligingsmaatregelen met als doel terrorismebestrijding is een activiteit die wordt uitgeoefend op basis van het openbaar gezag. Publieke betoelaging van dergelijke niet-economische activiteiten vallen in principe niet onder het staatssteunverbod van artikel 87 van het EG-verdrag. Er moet wel altijd gezorgd worden dat de ontvangen subsidies niet voor andere economische activiteiten worden aangewend. Overheidssteun die aangewend wordt voor de beveiliging door havenexploitanten, vervoersondernemingen of goederenbehandelaars vallen wel onder de staatssteunregels.

Dus zoals hierboven beschreven wordt, ontvangen de Vlaamse havenbesturen geen overheidssteun. Er zijn ook geen indicaties dat dit in de nabije toekomst zal veranderen. Indien er toch een overheidsfinanciering zal overwogen worden, moet er uitgemaakt worden of deze ten laste valt van de federale of van de Vlaamse regering. In het Belgische staatsrecht geldt de regel dat alleen die overheid welke voor de betrokken materie bevoegd is, deze materie mag financieren. (o.m. Raad van State, afdeling wetgeving, advies nummer 32.371/VR van 23 oktober 2001) Hierdoor is een eventuele financiering van havenbeveiliging een federale aangelegenheid. De Vlaamse overheid is bevoegd voor een aantal randaspecten, zoals de verwerking van de ISPS-gegevens in het raam van een verkeersbegeleidingssysteem (voorschrift 9) en de beveiliging van het verkeersbegeleidingssysteem zelf tegen terrorisme (B.15.7).

5.4.3 Doorrekening van beveiligingskosten in scheepvaartrechten en havengelden

Vele terminalexploitanten en rederijen heffen een speciale toeslag om de door hen gemaakte beveiligingskosten te dekken. Het is ook mogelijk dat waterweg- en havenbesturen voor de door hen gemaakte kosten een dergelijke toeslag zullen aanrekenen of een afzonderlijke taks invoeren. Hiervan zijn nog geen voorbeelden bekend. Allicht worden de bijkomende kosten opgenomen in de algemene budgetten en gefinancierd vanuit de algemene opbrengst van de (al dan niet verhoogde) havengelden. De eventuele doorrekening van de bijkomende kosten in de haventarieven is meestal niet traceerbaar.

Internationale randvoorwaarden

De aanrekening van kosten aan schepen wordt beperkt door het internationaal zeerecht. Tengevolge het VN Zeerechtverdrag en het internationaal gewoonterecht mogen in de territoriale zee alleen kosten in rekening worden gebracht ter vergoeding van specifiek aan de schepen verleende diensten. Tengevolge van internationale verdragen zijn een aantal internationale waterwegen vrij van heffingen, zoals de Schelde. Het Internationaal Zeehaveninstituut verbiedt bij de heffing van havengelden elke vlagdiscriminatie en eist de

voorafgaande publicatie van de tarieven (zie artikelen 2 en 4 van het Statuut van Genève van 9 december 1923 aangaande het internationaal regime der zeehavens). Indien de waterweg- of havenbesturen de havengelden willen verhogen of een speciale taks willen invoeren moeten ze rekening houden met deze bepalingen.

Europese randvoorwaarden

Als er een heffing wordt doorgevoerd moet er ook gelet worden op de volgende beginselen: vrij goederenverkeer, vrij verkeer van diensten en het mededingingsrecht. Qua vrij goederenverkeer zal alleen een heffing die geïnd wordt op de geloste of geladen goederen vallen onder de regels van het vrije goederenverkeer en niet een taks of toeslag op de schepen. Het beginsel vrij verkeer van diensten kan slechts beperkt worden door regelingen die hun rechtvaardiging vinden in dwingende redenen van algemeen belang en die van toepassing zijn op alle personen en ondernemingen die hun activiteit uitoefenen op het grondgebied van de lidstaat van ontvangst. Dus het beschermen van de openbare veiligheid kan een dergelijke dwingende reden zijn. Een maatregel gerelateerd aan de ISPS-code heeft als doel de openbare veiligheid te verhogen, dus een beperking van het vrije goederenverkeer door een taks ter financiering van deze maatregel kan gerechtvaardigd worden. Hierbij dient wel te worden opgemerkt dat de beveiligingstaks geen vorm van discriminatie mag inhouden. Bijvoorbeeld een taks mag niet resulteren in een discriminatie van buitenlandse reders of andere havengebruikers gebaseerd op nationaliteit. Ten slotte vallen activiteiten verbonden aan het openbare gezag buiten het mededingingsrecht. Hierdoor zijn heffingen die worden opgelegd aan de havengebruikers niet onderworpen aan het kartelverbod en het verbod van misbruik van machtspositie.

Belgische randvoorwaarden

In België is het zo dat havenbedrijven via het Havendecreet uitsluitend retributies mogen vorderen van de havengebruikers. Een retributie wordt doorgaans gedefinieerd als een heffing die een geldelijke vergoeding inhoudt voor bepaalde prestaties van een openbare dienst ten voordele van een individuele heffingsplichtige. En er moet een redelijke verhouding bestaan

tussen de kostprijs van de geleverde dienst en de gevorderde retributie. Verder stelt een deel van de Belgische rechtsleer dat een retributie ook de tegenprestatie moet zijn voor een dienst waarop uit eigen beweging een beroep is gedaan. Als we dit toepassen op de eventuele taksen die geheven worden omwille van de ISPS-code, dan kunnen er problemen ontstaan omdat er aangetoond zal moeten worden dat de havengebruiker zelf heeft gevraagd om de aangeboden diensten. Dit vormt geen probleem als men het woord vrijwilligheid laat vallen. De definitie stelt ook dat een retributie een vergoeding is voor een specifieke dienst verleend aan één gebruiker. Dus als er een taks geheven wordt, dan zal deze gelden voor alle gebruikers. Er kunnen hierover dus problemen ontstaan.

In het algemeen is het zo dat havenbedrijven de kosten kunnen recupereren door een verhoging van de havengelden, maar dat een specifieke toeslag ter dekking van deze kosten aangetast kan worden door het feit dat deze toeslag geldt voor alle gebruikers en niet voor één specifieke gebruiker.

5.4.4 Doorrekening van kosten in vracht- en behandelingsprijzen

Vele reders en terminalexploitanten spreken van een toeslag ter dekking van de kosten van beveiligingsmaatregelen. In de haven van Antwerpen rekenen de containerbehandelaars een toeslag aan van EUR 9 per geloste of geladen container. Voor conventioneel stukgoed geldt er een beveiligingstoeslag van EUR 0,60 per ton. Deze behandelingstoeslagen worden aangerekend aan de reder, en deze rekent ze verder door in zijn tarieven. Dus in de praktijk wordt deze kost van het beveiligen aangerekend aan de verlader. Op deze manier van werken bestaan echter een aantal bemerkingen. Ten eerste zeggen een aantal verladers dat de beveiligingstoeslagen een verdoken vorm van prijsverhogingen zijn omdat er geen investeringskost tegenover staat. Ten tweede vinden een aantal partijen dat de opbrengsten de kosten overtreffen. En dus vinden ze dat de beveiligingstoeslag niet volledig moet aangerekend worden.

Contractsvrijheid

Het aanrekenen van een beveiligingstoeslag maakt het voorwerp uit van contractsvrijheid. Dit wil zeggen dat de partijen vrij de toeslag kunnen overeenkomen (art. 1134 B.W.). Indien de klant de toeslag te hoog vindt, moet hij niet instemmen met het contract en kan hij zich tot een andere partij richten.

Europese randvoorwaarden

In sommige gevallen kan een beveiligingstoeslag niet in overeenstemming zijn met het Europees Gemeenschapsrecht. Dit is het geval wanneer de toeslag overdreven hoog of discriminerend is en misbruik van de machtspositie inhoudt. In het geval van misbruik van machtspositie moet worden aangetoond dat de reder of terminalexploitant over een machtspositie beschikt, wat gezien de hevige concurrentie en de mogelijkheden tot substitutie binnen en tussen havens bijna niet zal voorkomen.

Wat niet mag is een toeslag die het gevolg is van afspraken tussen ondernemingen. Dit kan voor problemen zorgen. De beveiligingstoeslag ligt voor concurrerende havens vaak op hetzelfde niveau en zelfs binnen één haven wordt vaak hetzelfde tarief toegepast. Er zou dus kunnen aangegeven worden dat de beveiligingstoeslagen er gekomen zijn na onderling overleg. De raad kan gegeven worden aan de reders en de terminalexploitanten om ervoor te zorgen dat hun beleid in verband met de toeslagen berust op objectieve kostengegevens van de eigen onderneming.

Belgische randvoorwaarden

In België geldt de wet tot bescherming van de economische mededinging. Een beveiligingstoeslag zal bezwaren oproepen als hij strijdig is met de eerlijke handelsgebruiken. Daarnaast kan de heffing van een toeslag worden aangevochten als deze berust op wilsgebreken (onder andere dwaling en bedrog)

5.4.5 Conclusies

Wanneer een systeem ter financiering van de beveiligingsmaatregelen wordt ingesteld, moet gelet worden op de volgende regels:

- Overheidsfinanciering van publieke taken in verband met havenbeveiliging maakt geen staatssteun uit in de zin van het E.G.-Verdrag
- Het Vlaamse Havendecreet biedt een beperkte basis voor een subsidiëring van beveiligingskosten.
- De recuperatie van kosten van havenbeveiliging via de havengelden moet voldoen aan een aantal randvoorwaarden (bijvoorbeeld het vrij verkeer van goederen)
- Het Belgisch recht bemoeilijkt de invoering van specifieke havengelden, maar laat wel een verhoging van de algemene havengelden toe
- Beveiligingstoeslagen door reders of terminalexploitanten zijn mogelijk omwille van de contractsvrijheid, maar deze mogen niet berusten op een misbruik van de machtspositie, een ondernemersafspraak, een oneerlijke handelspraktijk of een wilsgebrek

De internationale, Europese en Belgische regelgeving biedt geen specifiek juridisch kader voor financiering van beveiligingskosten. Daardoor dreigen rechtsonzekerheid, rechterlijke procedures en concurrentieverstoringen. Het is belangrijk dat een degelijk juridisch raamwerk zo spoedig mogelijk wordt opgesteld.

Hoofdstuk 6: ISPS-code voor schepen en andere initiatieven

6.1 De ISPS-code voor schepen

De ISPS-code maakt een onderscheid tussen maatregelen die geldig zijn voor schepen en maatregelen die gelden voor havenfaciliteiten. Deze maatregelen kunnen niet los van elkaar gezien worden. In de voorgaande hoofdstukken zijn vooral de verplichtingen besproken die de havenfaciliteiten werden opgelegd, alsook hun aanpak om conform te zijn met de ISPS-code. In de ISPS-code en Verordening 725/2004 zijn de verplichtingen voor de schepen terug te vinden. De relevante artikelen voor de scheepsveiligheid zijn artikelen 7, 8, 9, 12, 13 en 19 in deel A en in deel B kunnen de richtsnoeren gevonden worden in de artikelen 8, 9 en 13.

In hoofdstuk 2 werden de verschillende veiligheidsniveaus besproken die zowel een schip als een havenfaciliteit moeten kunnen instellen wanneer dit nodig zou blijken. Het kan soms voorvallen dat het schip en de havenfaciliteit op een verschillend niveau werkzaam zijn. Wanneer dit het geval is, moeten ze op elkaar worden afgestemd. Dit gebeurt op de volgende manier:

Situatie	**Actie**
Niveau terminal gelijk aan niveau schip	Geen
Niveau terminal hoger dan niveau schip	Veiligheidsniveau van het schip wordt opgehaald
Niveau terminal lager dan niveau schip	Terminal neemt extra maatregelen met veiligheidsverklaring

Figuur 8: Manier van afstemmen tussen een schip en een havenfaciliteit

Bron: Guido Van Meel, 2005

6.2 Europese initiatieven

Naast Verordening 725/2004 voor schepen en havenfaciliteiten zijn er nog andere initiatieven bedacht door de Europese Commissie. Deze worden in dit hoofdstuk besproken. Europa heeft de beveiliging van zijn havens in twee stappen voorzien. Eerst dus de beveiliging van de havenfaciliteiten en pas later de beveiliging van het hele havengebied. Hierdoor heeft Europa de Richtlijn 2005/65 uitgewerkt betreffende het verhogen van de veiligheid van havens en deze dient dus om de veiligheid van de gehele haven te verbeteren. Volgens de Europese Commissie vormen havens een risico omdat ze een essentiële link zijn binnen de totale vervoersketen en omdat ze handel- en passagiersstromen over zee en land met elkaar verbinden. Havens zijn vaak het knooppunt voor het overbrengen van gevaarlijke vracht, voor belangrijke chemische en petrochemische productiecentra, en/of ze zijn in de buurt van steden gelegen. Het is duidelijk dat terroristische aanslagen in havens kunnen resulteren in ernstige ontregelingen van de vervoerssystemen en domino-effecten kunnen teweegbrengen op de industrie aanwezig in de omgeving, alsook directe schade kunnen berokkenen aan mensen in de havens en aan de omwoners. Daarom heeft de Commissie deze Richtlijn betreffende de veiligheid van havens ontwikkeld.

Het verschil met Verordening 725/2004 is dat de Verordening rechtstreeks toepasselijk is in de lidstaten en bindend is in al zijn onderdelen, terwijl bij de EU-Richtlijn enkel het eindresultaat telt. Om het ganse havengebied te beveiligen mag elke lidstaat dus zelf bepalen op welke manier men dit het beste aangepakt. Het is de bedoeling dat tegen juni 2007 de beveiligingsmaatregelen van de Richtlijn aansluiten op de reeds bestaande beveiligingsmaatregelen van de Verordening 725/2004. De maatregelen van de Verordening hebben wel altijd voorrang op die van de Richtlijn.

De Richtlijn legt de verplichting op om een federale en (per zeehaven) lokale autoriteit voor havenveiligheid aan te duiden. Een eerste belangrijke taak van het lokale comité is het vaststellen van ‘gebieden met havenactiviteit’, aan de hand van gedetailleerde veiligheidsbeoordelingen. Verder moet voor het ganse havengebied een veiligheidsbeoordeling uitgevoerd worden, moet er een veiligheidsplan opgesteld worden en

tenslotte ook een havenveiligheidsfunctionaris aangeduid worden. De autoriteit voor havenveiligheid is verantwoordelijk voor de opstelling en de uitvoering van het havenveiligheidsplan. Dit plan wordt opgesteld op basis van de veiligheidsbeoordeling. Volgens artikel 6 van de Richtlijn moet deze beoordeling rekening houden met de specifieke kenmerken van de verschillende delen van de haven, desgevallend ook met de naburige gebieden indien deze een invloed kunnen hebben op de veiligheid in de haven en moet er rekening worden gehouden met de beoordelingen die werden uitgevoerd op basis van Verordening 725/2004. Na het opstellen van de veiligheidsbeoordeling moet het havenveiligheidsplan uitgewerkt worden. In dit plan moeten voor elk van de drie veiligheidsniveaus de te volgen procedures, de in te voeren maatregelen en de te nemen maatregelen worden vastgesteld. Bij de opstelling moet men rekening houden met de eisen zoals vermeld in bijlage II van de Richtlijn. Zo moet men onder andere taken specificeren en werkschema's toewijzen voor de volgende gebieden:

- Toegangseisen
- Identiteits-, bagage- en vrachtcontrole-eisen; deze kunnen verschillen per subgebied
- Procedures en maatregelen betreffende het omgaan met verdachte vracht, bagage, bunkering, enzovoort
- Controle-eisen voor subgebieden of activiteiten binnen subgebieden
- Communicatie- en veiligheidsmachtiging
- Melding van veiligheidsincidenten
- Integratie in andere preventieve plannen of activiteiten
- Opleidings- en oefeneisen
- Procedures voor het aanpassen en actualiseren van het havenveiligheidsplan

Om op deze Richtlijn in te spelen heeft de haven van Antwerpen een risicoanalyse van het ganse havengebied laten uitvoeren door MUSC (Maritime Underwater Security Consultants). Op dit rapport gaat het Havenbedrijf van Antwerpen inspelen. Ze gaan bekijken waar de beveiliging beter kan en ze gaan deze punten effectief aanpakken.

Is deze stapsgewijze aanpak van de Europese Commissie niet overbodig? De beveiliging van het hele havengebied kan toch op technisch en op financieel vlak een belangrijke impact

hebben op de beveiliging van de havenfaciliteiten. En is het wel een goed idee om elke lidstaat vrij te laten in de uitwerking van de beveiliging van het ganse havengebied. Het zou toch beter zijn moesten ook hier duidelijke standaarden worden vastgelegd door de Europese Commissie, zodat elke Europese haven op een uniforme manier wordt beveiligd. En zodat tevens de veiligheidsplannen van de havens op dezelfde manier worden opgebouwd.

Indien alle wetgeving van de ISPS-code wordt samengevat, bekomt men Figuur 9:

Figuur 9: Overzicht van de wetgeving in verband met de ISPS-code

Bron: Eigen verwerking

Daarnaast heeft de Europese Commissie een Voorstel tot Verordening COM 2006/79 betreffende een betere beveiliging van de bevoorradingsketen uitgevaardigd. In deze Verordening staan de doelstellingen te lezen en deze zijn:

- De beveiliging van de bevoorradingsketen verbeteren zonder belemmering van het vrije handelsverkeer
- Een gemeenschappelijk kader tot stand brengen voor een systematische Europese aanpak zonder de gemeenschappelijke vervoersmarkt en bestaande veiligheidsmaatregelen in het gedrang te brengen
- Vermijden van overbodige administratieve procedures en lasten op zowel Europees als lidstaatniveau

Om dit te kunnen garanderen stelt de Europese Commissie volgende richtlijnen voor:

- De invoering van een verplicht systeem waarbij de lidstaten een kwaliteitslabel dienen in te voeren voor 'veilige exploitanten' dat wordt toegekend aan bevoorradingsexploitanten die voldoen aan de Europese veiligheidsnormen en daarom door de andere lidstaten van de interne markt kan worden erkend
- De invoering, binnen de bindende bepalingen voor de lidstaten, van een vrijwillige regeling waarbij aan bevoorradingsexploitanten stimulansen worden geboden om hun veiligheidsprestaties te verbeteren
- De verantwoordelijkheid van de bevoorradingsexploitanten voor hun veiligheidsprestaties in het Europese goederenvervoer
- 'Veilige exploitanten' genieten faciliteiten bij de uitvoering van veiligheidscontroles en kunnen zich inzake veiligheid positief onderscheiden van andere concurrenten waardoor ze over een handels- en concurrentievoordeel beschikken
- Voorzien in de mogelijkheden van een regelmatige aanpassing en verbetering van de veiligheidsvoorschriften, met inbegrip van internationaal erkende normen en voorschriften, via de comitéprocedure

Bij deze Verordening dient opgemerkt te worden dat het nog altijd niet duidelijk wie verantwoordelijk is voor de beveiliging. Men moet dus nog uitmaken of één van de betrokken exploitanten verantwoordelijk moet zijn voor de hele bevoorradingsketen of dat elke exploitant verantwoordelijk is voor de beveiliging van zijn onderdeel van de keten.

Een laatste initiatief van de Europese Commissie wat betreft beveiliging is de Verordening COM/2003/0452 betreffende de rol van de douane in het geïntegreerde beheer van de buitengrenzen en de Paperless Douane en Accijnzen (PLDA). Voor de implementatie van deze elektronische douaneomgeving in Europa heeft de Europese Commissie een strategisch kader ontworpen. De implementatie verloopt dus over een aantal jaren zodat alle lidstaten de mogelijkheid krijgen om de nodige aanpassingen door te voeren. De lidstaten hebben zich verbonden tot het gebruik van elektronische douanesystemen voor meer performante douaneprocessen. De Europese Commissie streeft ernaar om de douane-inklaring efficiënter te laten verlopen, de administratieve lasten te verlagen en fraude en terrorisme te bestrijden.

In het voorgaande voorstel tot Verordening COM/2003/0452 werd het begrip AEO (Authorized Economic Operator) gelanceerd. Dit initiatief valt onder de bevoegdheid van de douane. De douane zal instaan voor het certificeren van een bedrijf. Het begrip AEO houdt in dat een bedrijf de status kan ontvangen van AEO. Dit statuut zal ondernemingen toelaten veel vlotter te werken aangezien zij door de douane erkend zullen zijn als bedrijven die al een sterke interne controle hanteren en aan hoge kwaliteitseisen voldoen. Hierdoor zullen deze bedrijven beduidend minder fysieke controles ondergaan en kunnen zij hun goederen vlotter door de logistieke keten sturen. Zij krijgen een zogenaamde 'green lane', waar als het ware alle verkeerslichten op groen staan en zij zonder oponthoud hun goederen kunnen transporteren.

6.3 Amerikaanse initiatieven

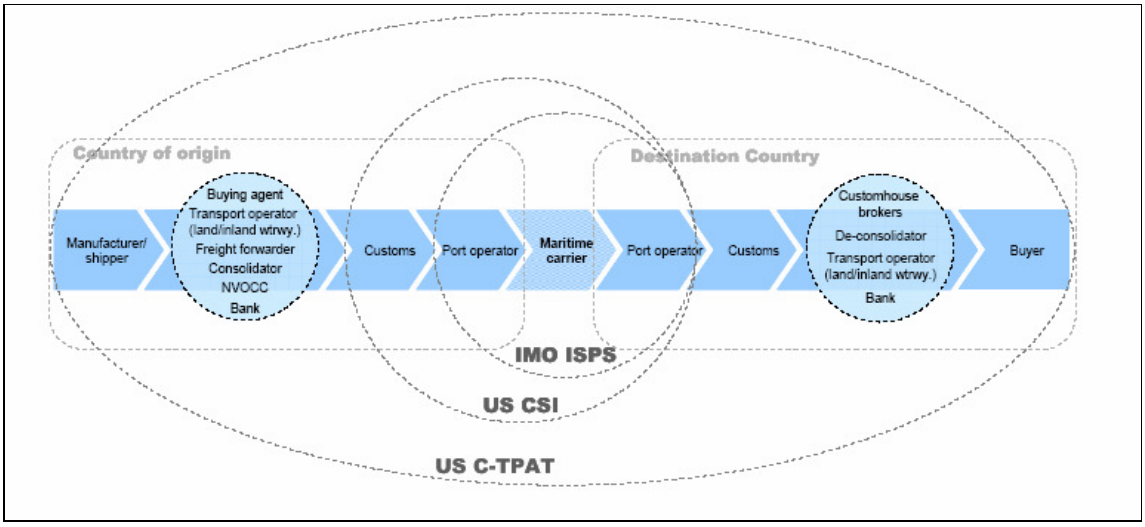
In tegenstelling tot Europa maakt de Maritime Transportation Security Act (MTSA) de ISPS-code in één keer toepasselijk op het hele havengebied in de Verenigde Staten.

Daarnaast zijn er nog drie andere Amerikaanse initiatieven aanwezig wat betreft het beveiligen van de logistieke keten waarbij de Verenigde Staten het volgende principe hanteren: 'to push out US virtual borders and stop suspicious containers before they leave their port of embarkation'. Dit wordt ook 'Second Line of Defense' genoemd.

Een eerste initiatief is het Container Security Initiative (CSI). De bedoeling hiervan is dat de goederen reeds gecontroleerd worden in de exporthaven en niet meer in de Amerikaanse havens. Hiervoor heeft Amerika bilaterale samenwerkingsakkoorden afgesloten met buitenlandse havens. De bepaling van welke goederen gecontroleerd zullen worden is afhankelijk van de resultaten van een risicoanalyse. De 24-uurs manifestregel is binnen het CSI-initiatief de belangrijkste richtlijn met verregaande administratieve implicaties. Dit betekent dat gedetailleerde informatie betreffende een lading 24 uur voor het laden in een vreemde laadhaven moet doorgestuurd worden aan de Amerikaanse douane. (Jacobs en Heuvelman, 2005) Het laatste initiatief is C-TPAT (Container Trade Partnership Against

Terrorism). Hiermee wil de Amerikaanse douane de volledige bevoorradingsketen beveiligen. Dit is een vrijwillig initiatief wat betekent dat rederijen, terminaloperators, exporteurs, enzovoort er zelf voor kiezen een vragenlijst van de douane in te vullen. Met deze vragenlijst geeft elk van hen informatie over de procedures van het bedrijf inzake interne controle. De douane kan vragen om bijkomende controlemaatregelen te nemen en dan beschouwt men het bedrijf als 'betrouwbare' partner.

Samengevat kan gezegd worden dat de ISPS-code, Verordening 725/2004, C-TPAT en CSI alle vier gericht zijn op het voorkomen van terroristische aanslagen op zeeschepen, de havenfaciliteiten die deze zeeschepen afhandelen en de goederen die verscheept worden. Op Figuur 10 wordt aangegeven welke partijen betrokken worden bij elk van de Amerikaanse initiatieven en de ISPS-code.



Figuur 10: Betrokken partijen bij de Amerikaanse initiatieven en de ISPS-code

Bron: OECD-studie, juli 2003

In Europa hebben de beveiligingsmaatregelen, die krachtens Verordening 725/2004 dienen genomen te worden, altijd voorrang op de beveiligingsmaatregelen van CSI en C-TPAT. Dit zal in de praktijk voor de nodige spanningen zorgen.

Daarnaast heeft Amerika ook de Bioterrorism Act of 2002 opgesteld. Deze maatregel heeft vooral invloed op de rederijen en de transportdragers. De bedoeling is om de voedselketen te beveiligen en daarom vraagt het FDA (Federal Food and Drug Administration) dat bepaalde informatie over de invoer van voedselproducten voor aankomst in de Verenigde Staten wordt gemeld. Daarnaast moeten de voedselproducenten en opslagfaciliteiten voor voedsel zich laten registeren bij het FDA en ze moeten een lokale verantwoordelijke aanduiden. Hierbij valt op te merken dat containerterminals die enkel containers behandelen en dus niet uitgerust zijn met koelhuizen of andere opslagplaatsen voor tijdelijke opslag niet onder deze wetgeving vallen. Meer informatie kan gevonden worden op de website van het FDA, www.cfsan.fda.gov (Van Meel, 2005)

Nog een belangrijk beveiligingsinitiatief dat zijn oorsprong vindt in Amerika is het 'Megaports Initiative' of MPI. Dit is een samenwerking tussen de National Nuclaer Security Administration (NNSA) en de douane (CPB, Customs and Border Protection) van de Verenigde Staten. Het MPI ondersteunt het Container Security Initiative (CSI). Binnen het kader van CSI heeft de Amerikaanse regering akkoorden gesloten met landen waarin zich havens bevinden die ten eerste voldoen aan bepaalde minimale standaarden en ten tweede een belangrijk volume aan containers verschepen naar de Verenigde Staten. MPI voorziet in die CSI-havens in de bijkomende installatie van apparatuur voor het detecteren van ongeoorloofd transport van nucleaire en radioactieve materialen die tegen de Verenigde Staten of tegen het gastland zouden kunnen gebruikt worden. De bedoeling van het akkoord is om 100% van het containerverkeer te controleren op ongeoorloofd transport van nucleaire en andere radioactieve materialen, om dit te doen bij zowel de invoer, de uitvoer als de doorvoer en dit in alle Belgische zeehavens, met Antwerpen als eerste te implementeren haven. Het akkoord werd afgesloten tussen enerzijds het Department of Energy (DOE) van de Verenigde Staten (in het bijzonder het NNSA) en anderzijds de Federale overheidsdienst Financiën van België (in het bijzonder de Administratie der douane en accijnzen). Andere partners die betrokken zijn bij dit initiatief zijn het Antwerps Havenbedrijf, de Antwerpse havengemeenschap, het Federaal Agentschap voor nucleaire controle, de NMBS en alle Antwerpse containerterminal operators. Tussen de Amerikaanse regering en de Belgische regering wordt een MOU (Memorandum of Understanding) ondertekend waarin de verantwoordelijkheden van beide

partijen worden vastgelegd. De Amerikaanse overheid staat in voor de volgende taken: aankoop van al het materiaal (onder andere detectiepoorten en computermateriaal), alle burgerlijk-bouwkundige werken (inclusief alle bijhorende administratieve daden zoals bouwvergunningen), opleiding van het personeel, indienststelling van de systemen en technische begeleiding in Antwerpen gedurende de eerste maanden, onderhoud gedurende de eerste drie jaren en het aanleggen van glasvezelbekabeling vanaf de detectiepoorten tot aan het netwerk van de Belgische douane. De Belgische overheid moet zorgen voor het inzetten van het personeel, het huren van het glasvezelnetwerk, het betalen van alle belastingen en het onderhoud van de toestellen na verloop van drie jaar te rekenen vanaf de indienststelling van de detectiepoorten. Belangrijk om op te merken is dat het grootste deel van de investeringen dus voor rekening van de Amerikaanse overheid is. Men schat de investeringen voor de Verenigde Staten gedurende de jaren 2005, 2006 en 2007 op EUR 11.250.000 en voor de Belgische overheid op EIR 2.583.000 De werkingskosten voor de Verenigde Staten zijn onbekend en voor België bedragen deze EUR 970.000 voor de drie jaren samen. (Persvoorstelling Administratie Douane & Accijnzen, 24 november 2004)

Een laatste initiatief is E-SEAL of Electronic Container Seal (ISO 18185). Dit initiatief is ontstaan omdat er zeer binnenkort een regelgeving zal komen vanuit het DHS (Department of Homeland Security, Verenigde Staten) dat van elke container die de Verenigde Staten binnenkomt de containerseal voor aankomst zal moeten gecontroleerd worden op zijn integriteit. Deze controle kan manueel gebeuren, maar kan ook automatisch als er gebruik gemaakt wordt van elektronische containerseals. Omwille hiervan hebben ‘solution-providers’ samen met de grootste rederijen en goederenbehandelaars het initiatief opgezet om een standaard op te zetten voor een ‘electronic seal’. De voordelen van deze elektronische seal zijn dat je op de ‘e-seal’ informatie kan wegschrijven met betrekking tot de logistieke goederenstroom van de desbetreffende container alsook over de relevante veiligheidsaspecten van de container. Ook tracking en tracing behoren tot de mogelijkheden. Dit kadert ook in de hele RFID-materie (zie verder).

6.4 Initiatieven aangestuurd vanuit de industrie

Momenteel zijn er in België vier initiatieven die aangestuurd worden vanuit de industrie. Deze zijn:

- Task Force Beveiliging Deurganckdok: het Deurganckdok is het nieuwe dok waar P&O Ports een containerterminal uitbaat en waar ook PSA een terminal uitbaat. De bedoeling is om voor het Deurganckdok een 'geïntegreerd beveiligingsconcept' te ontwikkelen en dus niet voor de twee terminals afzonderlijk een beveiligingsconcept uit te werken.
- RFID of Radio Frequency Identification: dit is een methode om van een afstand informatie op te slaan en te lezen van zogenaamde RFID-tags die op of in objecten zitten.
- Container Security Device (arming containers against intrusion): dit systeem is beveiligd tegen manipulatie en wordt in containers aangebracht en registreert elke opening van de containerdeur tijdens het internationale transport. Dit systeem wordt ontwikkeld door Commerceguard en dit is een samenwerking tussen Siemens en General Electric.
- ISO 20858 Maritime Port facility Security Assessments and Security Plan Development: dit biedt aan de havenfaciliteiten een hulpmiddel bij het uitvoeren van een risiscoanalyse (PFSA) en bij het opstellen van een veiligheidsplan (PFSP). Men biedt documentatie aan om er voor te zorgen dat de uitvoering op zo'n manier gebeurd dat het resultaat kan beoordeeld worden door de bevoegde autoriteit.

Deze initiatieven kaderen niet in een wetgevend kader. De betrokkenen zijn vrij om hun medewerking te verlenen aan deze initiatieven. In de praktijk zullen de 'solution-providers' of fabrikanten er proberen voor te zorgen dat hun oplossing de standaard zal worden en bijgevolg door de verschepers als een 'business qualifier' zal worden aanzien.

6.5 Initiatief van IMO (International Maritime Organisation) en ILO (International Labour Conference)

Er bestaat één beveiligingsinitiatief dat uitgaat van deze organisaties. Het gaat om Seafarers Identity Documents Convention 2003. De bedoeling van het dit initiatief is de beveiliging van het identiteitsbewijs van zeevarenden, om het zo het evenwicht te waarborgen tussen enerzijds de verbetering van de veiligheid in het zeevervoer en anderzijds de vereenvoudiging van de voorwaarden waaronder zeevarenden van boord van hun schip kunnen gaan in een land waarvan zij niet de nationaliteit hebben.

Hoofdstuk 7: Conclusies

De aanslagen op de WTC-torens in New York op 11 september 2001 betekende een hele verandering voor de wereld. Ook de transportsector kent sinds die dag talloze veranderingen. Die dag kwam het besef dat de logistieke keten gevoelig kan zijn voor terroristische acties. Een aanval op de keten kan immers zorgen voor de lamlegging van een land. Daarnaast kunnen terroristen de verschillende vervoersmodi gebruiken om het materiaal dat nodig voor een aanslag te verzenden. Het werd dus duidelijk dat de vervoerssector beter beschermd moest worden. Dat zou de enige manier zijn om terroristische acties te verhinderen en te vermijden.

De maritieme sector reageerde op de aanslagen van 11 september door een aanvulling op het bestaande SOLAS-verdrag uit te vaardigen, namelijk de ISPS-code. Elk van de 148 landen verbonden aan het SOLAS-verdrag moesten deze ISPS-code invoeren tegen één juli 2004. De bedoeling van de code is het opsporen van bedreigingen voor de veiligheid en het nemen van preventieve maatregelen tegen veiligheidsincidenten die de voor de internationale handel gebruikte schepen of havenfaciliteiten kunnen treffen. Onder een veiligheidsincident wordt verstaan: iedere verdachte handeling of omstandigheid die bedreigend is voor de veiligheid van een schip, een havenfaciliteit of het schip/haven raakvlak. Een mogelijke bedreiging is bijvoorbeeld het smokkelen van wapens, onbevoegde toegang, blokkeren van toegangen van een havenfaciliteit, enzovoort.

De ISPS-code bestaat uit twee delen, namelijk deel A en deel B. Deel A bevat de verplichtingen en deel B omvat de richtlijnen om te voldoen aan de verschillende verplichtingen. Europa heeft de ISPS-code overgenomen in Verordening 725/2004, maar om uniformiteit te garanderen heeft de Europese Commissie een aantal richtlijnen uit deel B eveneens verplichtend gemaakt. In België werd op 15 juni 2004 het Koninklijk Besluit tot oprichting van een federaal comité en lokale comités voor de beveiliging van de havenfaciliteiten uitgevaardigd. Dit Koninklijk Besluit houdt enkel het officialiseren van de controle- en overlegorganen in. Momenteel is de Belgische overheid aan het werken aan een wetsvoorstel betreffende maritieme beveiliging.

De ISPS-code maakt een onderscheid tussen drie beveiligingsniveaus. Het is aan de verdragsluitende staat om deze veiligheidsniveaus in te stellen en te communiceren naar de havenfaciliteiten. De havenfaciliteiten dienen dan gepast te reageren. Om dit doeltreffend te laten verlopen, zijn de havenfaciliteiten verplicht om een veiligheidsplan op te stellen. In dit veiligheidsplan worden de verschillende maatregelen besproken die van toepassing zijn bij elk veiligheidsniveau. De verantwoordelijkheid over deze maatregelen ligt bij de verdragsluitende staat. Voorschrift 10.3 van Verordening 725/2004 vermeldt immers dat de verdragsluitende staten de maatregelen per veiligheidsniveau dienen te communiceren aan de havenfaciliteiten. In België werden de zogenaamde 'sjablonen' uitgegeven om te voldoen aan deze verantwoordelijkheid. Deze sjablonen geven de maatregelen weer voor de gevoelige terminals, voor de niet-gevoelige terminals en de passagiersterminals en dit voor de verschillende veiligheidsniveaus. Maar de sjablonen komen niet overeen met de ISPS-code. Bijvoorbeeld het eerste sjabloon uitgevaardigd door het FCBH voor niet-gevoelige terminals is in strijd met artikel A.14.2 van Verordening 725/2004. Dit sjabloon geeft aan dat er geen beveiligingsmaatregelen dienen te worden genomen op veiligheidsniveau 1, terwijl artikel A.14.2 wel degelijk aangeeft dat er beveiligingsmaatregelen dienen te worden genomen. Bovendien zijn de door het FCBH voorgestelde beveiligingsmaatregelen in de sjablonen praktisch onuitvoerbaar en in strijd met artikel A.14.1 van Verordening 725/2004 waar duidelijk wordt aangegeven dat de beveiligingsmaatregelen geen vertragend effect mogen hebben.

Verordening 725/2004 haalt nog andere verantwoordelijkheden aan van de verdragsluitende staten en de havenfaciliteiten. De verdragsluitende staat moet zorgen voor de tenuitvoerlegging van de Verordening en voor de controle van de in de Verordening voorgeschreven veiligheidsmaatregelen. Verder moet de verdragsluitende staat aangeven wanneer er een veiligheidsverklaring vereist is en moet de verdragsluitende staat een 'Verklaring van naleving' afleveren. Tenslotte is de verdragsluitende staat verantwoordelijk voor het uitvoeren van een veiligheidsbeoordeling van de havenfaciliteiten. De havenfaciliteiten moeten een veiligheidsbeambte aanstellen en aanbevelingen doen om het veiligheidsplan bij te sturen. Een veiligheidsplan is immers een 'levend' document. Het is tevens aan de havenfaciliteiten om te zorgen voor de bescherming van de bedrijfsmiddelen en

de infrastructuur zoals de nutsvoorzieningen, het rollend materieel, enzovoort. Daarnaast moeten de havenfaciliteiten operationele veiligheidsmaatregelen treffen. Dit houdt bijvoorbeeld de toegang tot de havenfaciliteit in. Een laatste verplichting opgelegd aan de havenfaciliteiten is het organiseren van oefeningen. Via deze oefeningen kan een havenfaciliteit controleren of het veiligheidsplan optimaal werkt en kan het eventueel bijgestuurd worden.

De oefeningen die een havenfaciliteit moet houden zijn dus een manier om er voor te zorgen dat de ISPS-code gehandhaafd wordt. Er zijn ook nog andere mogelijkheden. Om er voor te zorgen dat onbevoegden geen toegang krijgen tot de havenfaciliteit of bepaalde gebieden van de havenfaciliteit is het noodzakelijk dat er een goede toegangscontrole bestaat. Op die manier kan ook gegarandeerd worden dat de beveiligingsmaatregelen nageleefd worden. In de haven van Antwerpen wordt gewerkt met de Alfapass. Elke frequente bezoeker van de haven kan een dergelijke pas aanvragen en de havenfaciliteiten kennen de toegangsrechten per kaarthouder toe. Op die manier kunnen ze controleren welke personen tot welke gebieden toegang hebben. Daarnaast biedt de Alfapass ook een voordeel indien er zou moeten geëvacueerd worden. De Alfapass registreert welke personen zich waar bevinden en hierdoor kan een effectieve evacuatie gebeuren. De Alfapass is een goed systeem omdat het drie belangrijke principes combineert. Deze principes zijn toegangscontrole, toegangsregistratie en het bevoegd verklaren (waar, wie en waarom).

Er kunnen controles uitgevoerd worden door de Europese Commissie zoals geregeld wordt door Verordening 884/2005. Deze controles dienen aangekondigd te worden en de verdragsluitende staat moet de volledige medewerking garanderen. De controleurs van de Europese Commissie stellen een verslag op en de verdragsluitende staat moet deze opmerkingen meedelen aan de havenfaciliteiten en/of schepen. Deze partijen moeten alles in het werk stellen om te voldoen aan de opmerkingen van de controleurs. De verdragsluitende staat moet een antwoord sturen op het verslag waarin aangegeven wordt op welke manier de havenfaciliteiten en/of schepen trachten te voldoen aan de opmerkingen en aanbevelingen. Momenteel kunnen er in België eveneens controles uitgevoerd worden door het federaal comité, als door de auditteams van de lokale comités. Het wetsvoorstel betreffende maritieme

beveiliging zou ook ambtenaren van het FOD Binnenlandse Zaken en het FOD Mobiliteit en Vervoer bevoegd verklaren voor deze controles. Deze ambtenaren zullen een beroep kunnen doen op de personeelsleden van de politiediensten om hen te helpen bij deze taak.

De andere bevoegdheden van het federaal comité en de lokale comités worden momenteel geregeld door het Koninklijk Besluit van 15 juni 2004. In de toekomst zal dit Koninklijk Besluit vervangen worden door het wetsvoorstel betreffende maritieme beveiliging. De bevoegdheden van de comités worden in het wetsvoorstel uitgebreid. De belangrijkste verantwoordelijkheid van het federaal comité is zorgen voor de algemene coördinatie van de beveiligingsmaatregelen voor de invoering van de nationale en internationale wetgeving. Het federaal comité is ook verantwoordelijk voor de goedkeuring van de veiligheidsbeoordelingen en de veiligheidsplannen. Het lokaal comité is bevoegd voor de controle van de echtheid van de geleverde inlichtingen door de havenfaciliteiten en de beoordeling van de veiligheidsplannen. Ze dienen alle gegevens eveneens op te volgen in de tijd. In deze comités zetelen verschillende leden, al dan niet met stemrecht. De expertise en de kennis van de havenfaciliteiten wordt niet gebruikt in de comités, maar er wordt wel overleg gepleegd. De bedoeling hiervan is om de havenfaciliteiten toch te betrekken bij de beslissingen, maar om ook op een vlotte manier knopen te kunnen doorhakken zonder rekening te moeten houden met de mening van elke havenfaciliteit. Een andere reden is dat met deze manier van werken de geheimhouding van bepaalde gegevens van de havenfaciliteiten wordt gewaarborgd.

Om in overeenstemming te zijn met de ISPS-code en eveneens aan Verordening 725/2004 zullen alle betrokken partijen een aantal investeringen moeten doen. Om een beter inzicht te krijgen in het totale kostenplaatje van de beveiligingsmaatregelen wil de Europese Commissie een studie hierover laten uitvoeren. Deze studie is tot op heden nog niet gebeurd, maar om toch een idee te krijgen over de kosten werd de studie van het OECD bestudeerd. In deze studie wordt een onderscheid gemaakt tussen de maatregelen op basis van de verantwoordelijke voor het instellen van de maatregel. Zo zijn er maatregelen die moeten geïmplementeerd worden door de overheid en maatregelen die van toepassing zijn op de rederijen en schepen of op de havenfaciliteiten. De conclusies van deze studie zijn vooral van toepassing op de Verenigde Staten, maar ze geven toch een beeld weer over de situatie in

andere landen. De kosten zijn berekend met gegevens van de Verenigde Staten zoals de loonkosten voor de beveiligingsbeambten. Deze kosten zullen verschillend zijn per land. Algemeen kan gezegd worden dat het invoeren van de beveiligingsmaatregelen voor alle partijen een aanzienlijke investeringskost met zich meebrengt Daarnaast zijn er ook de jaarlijkse onderhoudskosten voor bepaalde verplichtingen zoals de controle van het beveiligingsmateriaal.

De vraag die zich opdringt is natuurlijk wie de kosten van het hele beveiligingsgebeuren zal dragen. Er zijn een aantal mogelijkheden denkbaar zoals het verhogen van de havengelden zodat de havenbesturen hun kosten kunnen terugwinnen. Of het doorrekenen van de beveiligingskosten in de vracht- en behandelingsprijzen zodat de havenfaciliteiten de kosten kunnen recupereren. Een derde mogelijkheid is het krijgen van overheidssteun. In de Verenigde Staten werd het geven van overheidssteun geregeld in de wetgeving. In Europa zijn de overheden minder bereid om financiële steun te verlenen. Omdat er geen raamwerk aanwezig is, wordt er gevreesd voor concurrentievervalsing. Overheidssteun zou in alle landen van de Europese Unie op dezelfde manier moeten verlopen, maar er ontbreekt dus een goede regelgeving om dit te garanderen. Er is wel een mogelijkheid om staatssteun te krijgen voor niet-economische activiteiten die worden uitgeoefend op basis van het openbaar gezag, zoals bepaalde beveiligingsmaatregelen tegen terrorismebestrijding. Belangrijk hierbij is dat de verkregen steun niet wordt aangewend voor economische activiteiten. Indien er in België overheidssteun zou gegeven worden, moet uitgemaakt worden of dit ten laste komt van de federale of Vlaamse overheid. Het is zo dat de bevoegde overheid ook in staat voor de financiering. In België is de federale overheid bevoegd en zal dus moeten instaan voor de financiering.

De tweede mogelijkheid is het doorrekenen van de beveiligingskosten in de havengelden. Hiermee kunnen de havenbesturen of de waterwegbesturen de door hun gemaakte kosten terugwinnen. Een verhoging van de havengelden is onderworpen aan een aantal randvoorwaarden. Internationaal gelden er een aantal regels die voorschrijven dat alleen kosten in rekening mogen worden gebracht voor diensten die specifiek geleverd worden aan een schip. Verder geldt dat een aantal internationale waterwegen vrij zijn van heffingen en dat

een heffing nooit mag zorgen voor vlaggendiscriminatie. Indien de havenbesturen een heffing willen invoeren, moet er dus gelet worden op deze regels. Verder moet er binnen Europa rekening gehouden worden met drie principes. Ten eerste met het vrij verkeer van goederen, maar dit is enkel van toepassing op geladen en/of geloste goederen en dus niet op een heffing voor schepen. Ten tweede het vrije verkeer van diensten. Dit kan beperkt worden door regels die nodig zijn voor het algemeen belang. Een maatregel ter voorkoming van terrorisme kan hierdoor gerechtvaardigd worden. Ten derde moet gelet worden op het mededingingsrecht. Activiteiten verbonden aan het openbaar gezag vallen hier niet onder. Hierdoor kan een heffing opgelegd om de kosten van beveiliging te recupereren niet afgekeurd worden op basis van het mededingingsrecht. In België is het enkel toegestaan dat de havenbesturen retributies vorderen van de havengebruikers. Een retributie houdt in dat er een vergoeding bestaat voor een prestatie die geleverd werd door een openbare dienst aan een bepaalde heffingsplichtige. En verder moet de heffingsplichtige zelf gevraagd hebben om de geleverde prestatie. Dit levert problemen op indien het havenbestuur een dergelijke retributie wil invoeren, want er moet aangetoond worden dat de gebruikers gevraagd hebben achter de beveiligingsmaatregelen. Als er niet gekeken wordt naar de vraag van de heffingsplichtige zelf kunnen er nog problemen ontstaan, want een retributie is geldig voor één specifieke gebruiker en mag dus niet opgelegd worden aan alle havengebruikers.

Ten slotte kunnen de havenfaciliteiten de kosten terugwinnen door het invoeren van een beveiligingstoeslag. Dit heeft te maken met de contractsvrijheid en is in principe dus mogelijk. Er moet wel gelet worden dat de beveiligingstoeslag niet in overtreding is met het Europees Gemeenschapsrecht. Dit is het geval wanneer de toeslag te hoog of discriminerend is en misbruik van een machtspositie inhoudt. Het is ook niet toegelaten dat de havenfaciliteiten onderling afspraken maken over de beveiligingstoeslag. In België zal een toeslag niet geldig zijn als deze berust op wilsgebreken of als deze strijdig is met de eerlijke handelspraktijken.

In de praktijk kan vastgesteld worden dat de havenfaciliteiten een beveiligingstoeslag variërend tussen EUR 9 en EUR 10 per geloste en/of geladen container aanrekenen en voor conventioneel stukgoed geldt een toeslag van ongeveer 0,60 EUR per ton afhankelijk van de

aard en de verpakking van de goederen. De beveiligingstoeslag voor ‘general cargo’ kan echter sterk uiteenlopen. Er dient dus opgemerkt te worden dat de toeslagen voor wat betreft containers ongeveer in dezelfde lijn liggen voor de verschillende havenfaciliteiten. De havenfaciliteiten dienen er voor te zorgen dat ze kunnen aantonen dat deze toeslagen berekend zijn op objectieve kostengegevens van de eigen onderneming. Zo niet kan er geredeneerd worden dat de toeslagen er gekomen zijn na onderling overleg en dit maakt de beveiligingstoeslag ongeldig. Momenteel is er nog geen sprake van een verhoging van de havengelden. De havenbesturen gaan de kosten van de beveiliging opnemen in hun algemene budgetten en worden deze kosten gefinancierd vanuit de algemene opbrengsten. Zoals eerder aangehaald is er momenteel geen overheidssteun en er zijn ook geen indicaties dat er in de toekomst overheidssteun zal komen.

Naast de ISPS-code zijn er nog andere beveiligingsinitiatieven ontstaan. Vooral de Verenigde Staten eisen verdere maatregelen, maar ook binnen Europa ontstaan nieuwe initiatieven. Daarnaast stuurt eveneens de industrie aan op nieuwe maatregelen en heeft de IMO en de ILO een initiatief in het leven geroepen. Met al deze maatregelen proberen alle partijen de kans op een veiligheidsincident te beperken.

Een belangrijk initiatief genomen door de Europese Commissie is de richtlijn 2005/65 betreffende het verhogen van de veiligheid van havens. Daarnaast is er een Voorstel tot Verordening COM 2006/79 betreffende een betere beveiliging van de bevoorradingsketen uitgevaardigd.

In Amerika werd de ISPS-code onmiddellijk toepasbaar gemaakt op het hele havengebied. Daarnaast probeert Amerika ook de logistieke keten beter te beveiligen met initiatieven zoals CSI, C-TPAT en de 24-uurs manifestregel. Met deze maatregelen proberen de Verenigde Staten om verdachte containers en goederen op te sporen vooraleer ze op Amerikaans grondgebied terecht komen.

De initiatieven aangestuurd vanuit de industrie kaderen niet in een wetgevend kader. Hierdoor zijn de betrokkenen vrij om hun medewerking te verlenen. Een voorbeeld hiervan is

Container Security Device. Dit wordt ontwikkeld door Commerceguard en dit systeem registreert elke opening van de container tijdens het internationale transport.

Het initiatief van IMO en ILO is het Seafarers Identity Documents Convention 2003. De bedoeling hiervan is het vinden van een goed evenwicht tussen het beveiligen van het zeevervoer en het eenvoudiger maken voor zeevarenden om aan land te gaan in een land waarvan ze niet de nationaliteit hebben.

Om een beter inzicht te krijgen in de hele materie en om de omzetting van theorie naar praktijk te kunnen maken, is er samengewerkt met P&O Ports. P&O Ports is één van de havenfaciliteiten in de haven van Antwerpen die zich in regel moest stellen met de ISPS-code en dus Verordening 725/2004 en de andere beveiligingsinitiatieven. Het bedrijf heeft zoals verplicht door de ISPS-code een veiligheidsbeambte in dienst genomen en een veiligheidsplan opgesteld voor de havenfaciliteit. Verder probeert het bedrijf er voor te zorgen dat de beveiligingsmaatregelen nageleefd en gehandhaafd worden. Er worden oefeningen gehouden om het veiligheidsplan bij te sturen en er wordt gebruik gemaakt van de Alfapass om een goede toegangscontrole te garanderen. Om de kosten terug te winnen vraagt P&O Ports aan zijn klanten een beveiligingstoeslag zowel voor containers als voor stukgoed. Deze kosten kunnen niet vrijgegeven worden, aangezien deze confidentieel zijn. Volgens P&O Ports kunnen er bij de OECD-studie een aantal vraagtekens geplaatst worden. Er worden een aantal kosten te hoog geschat zoals de kosten voor de overheid. Andere kosten worden dan weer te laag geschat zoals de kosten voor de havenfaciliteiten. De studie neemt te weinig kostenrubrieken op om de kosten van de havenfaciliteiten te bepalen, waardoor het cijfer bijgevolg te laag komt te liggen.

De gevolgen op lange termijn zijn moeilijk te voorspellen. Er dienen nog een aantal andere beveiligingsinitiatieven geïmplementeerd te worden en de vraag die dan dient gesteld te worden is: ‘Zijn al deze initiatieven wel nodig?’ Er moet gelet worden op de efficiëntie van de beveiligingsmaatregelen en er moeten niet zo maar tal van initiatieven genomen worden. Het is beter om in de werkelijkheid een goed draaiend systeem te hebben dat zorgt voor

beveiliging dan tal van mooie initiatieven op papier, maar die niets opleveren. In veel gevallen wordt er een gevoel van 'schijnveiligheid' opgewekt.

Er dient opgemerkt te worden dat er momenteel een te groot verschil bestaat tussen de theorie en de praktijk. Hierdoor is er nog steeds geen effectieve beveiliging in verschillende havenfaciliteiten. Om dit te verhelpen zal de Belgische overheid zich bewust moeten worden van de toegekende verantwoordelijkheden en de nodige maatregelen moeten meedelen aan de havenfaciliteiten. Zoals al een aantal keer werd aangehaald in deze eindverhandeling legt Verordening 725/2004 in voorschrift 10.3 vast dat de verdragsluitende staat aan de havenfaciliteiten moet meedelen welke maatregelen genomen moeten worden bij elk veiligheidsniveau. Dit is in België gebeurd via de zogenaamde 'sjablonen', maar deze zijn ontoereikend en niet conform Verordening 725/2004. Een ander voorbeeld dat de Belgische overheid zich niet bewust is van zijn verantwoordelijkheden is het feit dat de veiligheidsbeoordeling niet werd uitgevoerd. Dit is nochtans ook verplicht volgens hetzelfde voorschrift 10.3. De havenfaciliteiten hebben deze taak zelf uitgevoerd. Het is dus duidelijk dat de synergie die Verordening 725/2004 beoogt tussen de overheid en de havenfaciliteiten niet bereikt wordt. Dit blijkt ook duidelijk uit het gegeven dat de overheid geen medewerking wil verlenen voor de uitvoering van de oefeningen opgelegd door Verordening 725/2004. De vrees die leeft bij de havenfaciliteiten is dat zij hier (financieel) de dupe van kunnen worden wanneer er zich echt een crisissituatie zal voordoen. Door het niet inoefenen van crisissituaties kan er immers geen zekerheid gegeven worden dat een veiligheidsplan of een evacuatieplan ook echt werkt. Een ander voorbeeld van het ontbreken van synergie is dat het LOVECO elk gerapporteerd veiligheidsincident dient te onderzoeken. Tot op heden heeft P&O Ports 230 van dergelijke veiligheidsincidenten gemeld, maar van terugkoppeling is in de meeste gevallen geen sprake.

Door de laattijdige aandacht van de overheid voor het beveiligingsgebeuren werden veel havenfaciliteiten enkel op papier gecontroleerd. Dit zorgt ervoor dat deze havenfaciliteiten op papier wel conform de Verordening werken, maar in de werkelijkheid is hier niets van te merken. Hier dient opgemerkt te worden dat dit kan leiden tot concurrentievervalsing. Elke havenfaciliteit vraagt immers dezelfde beveiligingstoeslag, maar ze maken niet allemaal

dezelfde kosten. P&O Ports heeft op een professionele manier invulling gegeven aan Verordening 725/2004 en heeft dus de nodige investeringen gedaan. Verder heeft P&O Ports ook jaarlijks kosten voor beveiliging. P&O Ports ontvangt de beveiligingstoeslag, maar ze gebruiken deze toeslag effectief voor het dekken van de gemaakte kosten voor een betere beveiliging. Wordt P&O Ports dan niet benadeeld ten opzichte van concurrerende havenfaciliteiten die enkel op papier aan beveiliging doen? Wat hier bij aansluit is dat er nergens richtlijnen gekomen zijn van de Belgische overheid om er voor te zorgen dat de beveiligingsmaatregelen op een uniforme manier worden doorgevoerd. Een voorbeeld kan dit verduidelijken: er zal rond elke havenfaciliteit prikkeldraad geplaatst moeten worden om ervoor te zorgen dat er geen ongewenste personen de havenfaciliteit betreden. Momenteel zijn er geen richtlijnen over welk soort prikkeldraad dit moet zijn, over hoe hoog deze prikkeldraad geplaatst moet worden, enzovoort. Op deze manier kunnen de havenfaciliteiten ook onderhevig zijn aan concurrentievervalsing. Een suggestie naar de Belgische overheid is om te zorgen voor een uniforme regelgeving op dit gebied. Zo kan elke havenfaciliteit er zeker van zijn dat de concurrenten dezelfde kosten maken. Verder is het belangrijk dat de bevoegde autoriteiten snel beginnen met het controleren van de havenfaciliteiten. Het bestaande spanningsveld tussen ‘formal compliance’ en ‘physical compliance’ moet opgeheven worden. Beveiliging is nodig, maar is enkel nuttig als in de praktijk de nodige maatregelen genomen worden. Geen enkele partij heeft iets aan beveiliging op papier. De gevolgen van deze situatie zijn niet te overzien indien er eens echt iets fout loopt.

Nu de beveiliging van de schepen en de havenfaciliteiten doorgevoerd is, staat Europa voor een volgende uitdaging, namelijk het beveiligen van het ganse havengebied en later van de gehele logistieke keten. Om dit tot een goed einde te brengen zal de Belgische overheid zich beter bewust moeten worden van haar verantwoordelijkheden. Een pro-actieve aanpak is vereist. De overheid zal sneller de nodige autoriteiten moeten aanduiden en de bevoegdheden van de verschillende partijen vastleggen. Verder zullen de nodige controles moeten uitgevoerd worden om te vermijden dat er weer een groot verschil ontstaat tussen de theorie en de praktijk.

Op dit ogenblik werkt de Belgische overheid aan een wetsvoorstel betreffende maritieme beveiliging. In dit wetsvoorstel worden de ambtenaren van FOD Binnenlandse Zaken en FOD Mobiliteit en Vervoer bevoegd verklaard voor het uitvoeren van controles. De bedenking hierbij is of deze mensen wel de nodige specifieke kennis hebben om nalatigheden op te sporen. Tijdens het schrijven van deze eindverhandeling werd duidelijk hoe complex de hele materie is. De wetgeving zal nog complexer worden als de hele haven beveiligd wordt en later de gehele logistieke keten. Zullen deze ambtenaren de nodige opleidingen krijgen om hun job naar behoren uit te voeren? Verder worden in dit wetsvoorstel administratieve en strafrechterlijke sancties opgelegd aan havenfaciliteiten of havens die niet handelen volgens de regelgeving. Een bedenking die hierbij gemaakt kan worden, is hoe de Belgische overheid straffen kan voorzien zonder op een goede manier te hebben aangegeven wat de havenfaciliteiten moeten doen. Dit komt weer terug op voorschrift 10.3 van Verordening 725/2004 en de 'sjablonen'.

In het recent verschenen artikel 'Holes revealed in Europe's port security' (20 april 2006) wordt aangehaald dat de beveiliging bij veel havenfaciliteiten niet verloopt zoals het zou moeten. Verder wordt geschreven dat de overheden en de industrie dit gegeven niet openbaar willen maken omdat ze vrezen voor de economische impact hiervan op het goederenverkeer in de haven. In het artikel wordt eveneens vermeld dat de verzekeringspremies niet dalen en dat hierdoor een gebrek aan inzet verweten kan worden. Weer kan dus opgemerkt worden dat alle partijen hun verantwoordelijkheden moeten opnemen en dat er dringend nood is aan zowel een uniforme implementatie van de door Verordening 725/2004 opgelegde beveiligingsmaatregelen als aan fysieke controles en dus niet enkel controles op papier.

Er is dus duidelijk nog werk aan de winkel om een goede maritieme beveiliging uit te bouwen. Dit moet lukken in de toekomst als alle partijen zich bewust worden van het belang hiervan en hun verplichtingen effectief nakomen. Op deze manier kunnen drama's zoals 9/11 vermeden worden en blijven de commerciële belangen van de Belgische havenfaciliteiten gevrijwaard.

Lijst met geraadpleegde werken

Boeken

Witlox, F., *Beveiliging in het vrachtvervoer; mythe, macht of noodzaak?*, Garant, Antwerpen, 2005, 200 pp.

Artikels

NN (2006), 'Holes revealed in Europe's port security, *Fairplay International Shipping Weekly*, p. 13

Studies

Security in maritime transport: Risk factors and economic impact, Organisation for Economic Co-operation and Development, july 2003

Paperless douane en accijnzen business case, VIL-studie in opdracht van FOD Financiën, Administratie der douane en accijnzen, 2005

Websites

http://www.secure-marine.com/ISPS-2003.pdf [12/02/06]

http://www.poports.com [23/03/2006]

http://www.portofamsterdam.com [02/04/2006]

http://www.havenbeveiliging.be [04/04/2006]

http://www.portofantwerp.be/html/00_home/main_set_SO.html [05/04/2006]

http://www.mandusc.com/index.cfm [05/04/2006]

http://www.bihb.be [05/04/2006]

http://www.group4falck.be [05/04/2006]

http://gisis.imo.org/Public/ [06/04/2006]

http://www.portofantwerp.be [12/04/2006]

http://www.vil.be [13/04/2006]

http://www.cfsan.fda.gov [14/04/2006]

http://www.siemens.com [16/04/2006]

http://www.alfapass.be [02/05/2006]

http://www.imo.org [15/05/2006]

Wetteksten

Verordening (EG) nr. 725/2005 van het Europees Parlement en de Raad van 31 maart 2004 betreffende de verbetering van de beveiliging van schepen en havens, Publicatieblad van de Europese Unie, 29 april 2004

Koninklijk Besluit tot oprichting van een federaal comité en lokale comités voor de beveiliging van de havenfaciliteiten, Belgisch Staatsblad, 15 juni 2004

Richtlijn 2005/65/EG van het Europees Parlement en de Raad van 26 oktober 2005 betreffende het verhogen van de veiligheid van havens, Publicatieblad van de Europese Unie, 25 november 2005

Voorstel voor een Verordening van Europees Parlement en de Raad betreffende een betere beveiliging van de bevoorradingsketen, 27 februari 2006

Verordening (EG) nr. 884/2005 van de Commissie van 10 juni 2005 tot vaststelling van procedures voor inspecties van de Commissie op het gebied van maritieme beveiliging, Publicatieblad van de Europese Unie, 11 juni 2006

Wetsvoorstel betreffende maritieme beveiliging, 2006

Voorstel voor een beschikking van de raad waarbij de lidstaten worden gemachtigd in het belang van de Europese Gemeenschap het Verdrag van de Internationale Arbeidsorganisatie betreffende de identiteitsbewijzen van zeevarenden (verdrag nr. 185) te bekrachtigen

Andere

Persvoorstelling Administratie Douane & Accijnzen, 24 november 2004

Lijst met figuren

Lijst met tabellen

Lijst met afkortingen

AAPA	American Association of Port Authorities
AEO	Authorized Economic Operator
AIS	Automatisch Identificatiesysteem
BIHB	Beroepsinstituut voor Informatica, Haven en Beheer van goederenstromen
CBP	Customs and Border Protection
CCTV	Closed Circuit Television
CEPA	Centrale der Werkgevers aan de Haven van Antwerpen
CSI	Container Security Initiative
CSO	Company Security Officer
C-TPAT	Container Trade Partnership Against Terrorism
DHS	Department of Homeland Security
DOE	Department of Energy
EMSA	Europees Martitiem Veiligheidsagentschap
ESA	Equivalent Security Arrangement
E-SEAL	Electronic Container Seal
FCBH	Federaal Comité voor de Beveiliging van Havenfaciliteiten
FDA	Federal Food and Drug Administration
FOD	Federale Overheidsdienst
ILO	International Labour Conference
IMO	International Maritime Organisation, Internationale Maritieme Organisatie
ISPS-code	International Ship and Port facility Security code
KPI	Key Performance Indicator
LOVECO	Lokaal Veiligheidscomité voor de Beveiliging van Havenfaciliteiten
MOU	Memorandum of Understanding
MPI	Megaports Initiative
MTSA	Maritime Transportation Security Act

MUSC	Marine and Underwater Security Consultants
NNSA	National Nuclaer Security Administration
OECD	Organisation for Economic Co-operation and Development
OCR	Optical Character Recognition
PFSA	Port Facility Security Assessment
PFSO	Port Facility Security Officer
PFSP	Port Facility Security Plan
PFSS	Port Facility Security Staff
PLDA	Paperless Douane en Accijnzen
RFID	Radio Frequency Identification
RSO	Recognised Security Organisation
SOLAS	Safety of Life at Sea
SSA	Ship Security Assessment
SSO	Ship Security Officer
SSP	Ship Security Plan

Bijlagen

Bijlage 1: Interessante links

Bijlage 2: Contactgegevens van organisaties die opleidingen aanbieden

Bijlage 1: Interessante links

Verordening 725/2004 van het Europees Parlement en de Raad van 31 maart 2004 betreffende de verbetering van de havenbeveiliging van schepen en havenfaciliteiten kan geraadpleegd worden op EUR-Lex:
http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:52004PC0076:NL:NOT

Koninklijk Besluit van 15 juni 2004 tot oprichting van een federaal comité en lokale comités voor de beveiliging van de havenfaciliteiten kan geraadpleegd worden op de website van het Belgisch Staatsblad: http://www.ejustice.just.fgov.be/cgi/welcome.pl

De 'sjablonen' uitgevaardigd door het federaal comité (FCBH) kunnen geraadpleegd worden op de website van de haven van Gent: http://www.gabinfo.net/ (onder bibliotheek)

Het gewijzigd voorstel voor een Richtlijn van het Europees Parlement en van de Raad betreffende het verhogen van de veiligheid van havens kan geraadpleegd worden op EUR-lex: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52004PC0393:NL:HTML

Ook de andere aangehaalde Verordeningen uitgevaardigd door de Europese Commissie kunnen geraadpleegd worden op EUR-Lex

Bijlage 2: Contactgegevens van organisaties die opleidingen aanbieden

Group 4 Traning nv
Relegemstestraat 40 blok 44
1731 Asse
tel. 02/451.62.00
fax. 02/451.62.01
contact: ronald.engels@group4falck.be
www.group4falck.be

Hogere Zeevaartschool
Patrick Blondé
Noordkasteel Oost 6
2030 Antwerpen
tel. 03/205.64.30
fax. 03/225.06.39
contact: patrick.blonde@hzs.be

BIHB
Liesbeth Van den Wijngaert
Brouwersvliet 33 bus 8
2000 Antwerpen
tel. 03/205.18.87
fax. 03/231.67.28
contact: info@bihb.be

Marine Underwater Security Consultants
Chris Austen
Temple Stairs – Victoria Embankment
WC2R 2PN London
UK
tel. +44.20.7240.2663
fax. +44.20.7240.2663
contact: admin@uscl.co.uk

Renful Training Department
7 Aprey Gardens
WC2R 2RH London
UK
tel. +44.20.8457.9111
fax. +44.20.8457.9222
contact: mc4renful@aol.com
www.renful.com

Auteursrechterlijke overeenkomst

Opdat de Universiteit Hasselt uw eindverhandeling wereldwijd kan reproduceren, vertalen en distribueren is uw akkoord voor deze overeenkomst noodzakelijk. Gelieve de tijd te nemen om deze overeenkomst door te nemen en uw akkoord te verlenen.

Ik/wij verlenen het wereldwijde auteursrecht voor de ingediende eindverhandeling:
Beveiliging in de haven van Antwerpen : een bedrijfseconomische analyse
Richting: **Handelsingenieur** Jaar: **2006**
in alle mogelijke mediaformaten, - bestaande en in de toekomst te ontwikkelen - , aan de Universiteit Hasselt.

Deze toekenning van het auteursrecht aan de Universiteit Hasselt houdt in dat ik/wij als auteur de eindverhandeling, - in zijn geheel of gedeeltelijk -, vrij kan reproduceren, (her)publiceren of distribueren zonder de toelating te moeten verkrijgen van de Universiteit Hasselt.

U bevestigt dat de eindverhandeling uw origineel werk is, en dat u het recht heeft om de rechten te verlenen die in deze overeenkomst worden beschreven. U verklaart tevens dat de eindverhandeling, naar uw weten, het auteursrecht van anderen niet overtreedt.

U verklaart tevens dat u voor het materiaal in de eindverhandeling dat beschermd wordt door het auteursrecht, de nodige toelatingen hebt verkregen zodat u deze ook aan de Universiteit Hasselt kan overdragen en dat dit duidelijk in de tekst en inhoud van de eindverhandeling werd genotificeerd.

Universiteit Hasselt zal u als auteur(s) van de eindverhandeling identificeren en zal geen wijzigingen aanbrengen aan de eindverhandeling, uitgezonderd deze toegelaten door deze licentie

Ik ga akkoord,

Shana HOES

Datum: