Cyber, sea and risico's

Daniel SERVATY
Secretaris-generaal van de Koninklijke Belgische Marine Academie
Kapitein-ter-Zee (R)

Inleiding

De samenleving wordt meer en meer paperless, internationaler en virtueler. Transacties konden vroegen enkel bewezen worden of juridisch afdwingbaar of tegenstelbaar gemaakt worden indien ze werden vastgelegd op papier. In veel gevallen zelfs enkel bij wijze van authentieke akte door de tussenkomst van een notaris of ander openbaar ambtenaar [1] Onderhandse akten waren tussen burgers verplicht voor zaken waarvan de waarde de 3,000 Belgische franken overtrof. Enkel onder de 3,000 Belgische franken was het bewijs door getuigen toegelaten. Reeds toen lieten het Burgerlijk wetboek en het wetboek van koophandel tussen kooplui bewijs toe op een minder formalistische manier.

De snelle evolutie van schriftelijke communicatie op afstand gaande van de telegraaf over de telex die haar zwanenzang reeds beleefde in de jaren '80 van de vorige eeuw en nu voor de meeste mensen een onbekende is of herinnerd wordt als een oubollig, traag en complex communicatiemiddel. Het was echter een noodzakelijk kwaad en het beste middel om snel met een begin van bewijs internationaal te communiceren en handel te drijven.

Midden jaren '80 van de vorige eeuw maakte de telefax haar opwachting met haar eigen voordelen (teksten dienden niet volledig overgetikt te worden, vermindering van risico op fouten, handtekeningen en

---

1. Cfr ons goede oude burgerlijke wetboek art. 1315 & v. inzake het bewijs van verbintenissen.

aanpassingen konden snel van de éne zijde van de wereld met de andere worden uitgewisseld worden) en nadelen (het papier van de eerste faxrollen was niet stabiel en men moest veiligheidshalve kopies nemen van de ontvangen documenten omdat het origineel na verloop van tijd vervaagde of zelfs totaal onleesbaar werd. In het begin had men buiten een merkteken op het verzonden document ook geen enkel bewijs dat het document wel degelijk was verstuurd. Het juiste tijdstip kon niet onomstotelijk bewezen worden evenals dat de bestemmeling het document wel degelijk (volledig) had ontvangen.)

Hoe razend populair en gesofisticeerd de fax ook was (in een laatste fase was faxen vanuit de eigen laptop geen enkel probleem), en hoewel op briefpapier en business cards nog steeds faxnummers worden vermeld, neemt het gebruik ervan drastisch af.

Begin jaren '90 maakt de e-mail (en het internet) haar opwachting. In het begin voorbehouden voor de "happy few" en beperkt tot een "replication" per dag, heeft het een vlucht genomen die niemand op dat moment maar kon vermoeden.

De grote verschillen tussen e-mail en de vorige besproken schriftelijke communicatiemiddelen zijn het gemak, de snelheid waarmee met behoud van een spoor/begin van bewijs informatie kan uitgewisseld worden. Men is niet gebonden aan mainframes, desktops, pc's, zelfs niet eens laptops of tablets maar enkele standaard gsm kan dit aan én de info blijft ergens bewaard.

Waar computers in de jaren '70 voorbehouden waren voor top-bedrijven in airconditioned zalen, in de jaren '80 toegankelijk werden voor KMO's, zijn ze nu dermate geminiaturiseerd, geëxplodeerd in snelheid en capaciteit, mogelijkheid tot (betaalbare) connectie dat ze in het bereik liggen van iedereen, ongeacht leeftijd, ras of stand.

Het gaat dus niet alleen om communicatie maar om het opslaan, bewaren, beheren en mogelijk opnieuw exploiteren van gegevens, berichten en bestanden.

Transacties, financiële en andere zijn nu internationaal mogelijk in real time en wereldwijd. Ze vergroten de snelheid en mogelijkheden van de handel maar compliceren door hun snelheid en internationaal karakter gigantisch het juridisch kader dat hieraan niet is aangepast en ook moeilijk

in één welbepaald land of wetgeving kan gesitueerd worden. Alleen al daarom is het nodig om internationale afspraken te maken en samenwerkingen op punt te stellen.

De technologische evolutie is daarenboven zo snel dat wetgeving en regelgeving onmogelijk kan volgen. Het stelt de rechtzoekenden en rechters voor gigantische problemen: toepasselijk recht, bevoegdheid, gebrek aan kennis om bepaalde zeer technische dossiers te kunnen beoordelen en voeling houden met een cyber wereld die niet de hunne is maar die ze moeten gieten en beoordelen in een juridisch kader dat hieraan nooit heeft gedacht.

I. Wat is cyber ?

Cyber is in het Engels feitelijk geen zelfstandig naamwoord maar een adjectief. Het woord "cyber" zou dus bijgevolg steeds moeten gevolgd worden door een zelfstandig naamwoord bvb "cyber crime" [i1] Het is de afkorting van "cybernetics"[2], woord dat haar oorsprong vindt in de jaren '80 en slaat op de wetenschap van communicatie en automatisatie van controlesystemen van machines.

We zullen verderop zien dat het belangrijk is goed te begrijpen wat we precies met "cyber" bedoelen.

In de context van deze paper hebben we het over elektronische data, systemen en netwerken die gegevens verwerken en beheren maar ook verbanden leggen met toestellen, machines en tuigen en deze aansturen en controleren.

---

1. Relating to or characteristic of the culture of computers, information technology, and virtual reality:*the cyber age*
   http://www.oxforddictionaries.com/definition/english/cyber
2. The science of communications and automatic control systems in both machines and living things.
   http://www.oxforddictionaries.com/definition/english/cybernetics

II. Wat zijn de risico's verbonden aan cyber ?

We stelden hoger reeds dat de technische mogelijkheden en snelheid van computers en elektronische (kleine en draadloze) toestellen die data verwerken gigantisch zijn toegenomen en de praktische toepassingen ervan nemen nog dagelijks toe.

Denk maar aan alles wat te maken heeft met domotica, draadloze in real-time financiële verrichtingen, aankopen en transacties via het net, verwerken en uitbaten van (persoons)gegevens, aansturen van toestellen, automatisatie, enz.

Indien we de specialisten mogen geloven, staan we slechts aan de vooravond van een nieuwe evolutie die ongekende mogelijkheden biedt en de samenleving totaal zal hertekenen. Vermits we ons amper een idee kunnen vormen van het impact van deze wijzigingen op onze samenleving, hebben we parallel daarmee amper een idee van de daarmee samenhangende nieuwe risico's en problemen: Om maar enkele voorbeelden te geven: schepen en vaartuigen allerlei varen reeds jaren op elektronische kaarten, in het verlengde daarvan zijn onbemande bruggen, zelfs onbemande vaartuigen hoewel niet voor onmiddellijk (herinner je het juridisch kader: risico's, bevoegdheid en aansprakelijkheden). Hetzelfde geldt voor magazijnen waar volautomatisch goederen en colli in en uit rekken worden gehaald, zendingen worden voorbereid voor verscheping, in real time stock beheer dat met een onvoorstelbaar aantal parameters rekening kan houden[1], onbemande straddle carriers en portaalkranen die continu containerschepen laden en lossen, rekening houden met parameters zoals gewicht, gevarenklasse, volgende havens, haven van lossing, stabiliteit en veiligheid van het schip, efficiëntie (zo

---

1. Cfr studie van het VIL: Tracking & Tracing was een vijftal jaren geleden nog high tech : baanvervoerders implementeerden het om vrachtwagens met hoogwaardige en diefstalgevoelige lading zo goed als mogelijk te kunnen volgen. Colli-bedrijven hanteerden scanning om de stroom van hun pakjes te kunnen volgen en te kunnen pin-pointen waar colli verdwenen. Nu zijn de prijzen van de technologie voor RFID-tags (radio frequency identification) dermate gedaald en mogelijkheden zo toegenomen dat textielbedrijven de beschikbaarheid en locatie van kledingstukken kunnen identificeren tot op het model, de maat en de kleur. Cfr www.VIL.be

weinig mogelijk containers moeten lossen en herladen om één bepaalde container te kunnen behandelen), het positioneren van containers op de terminal, voorbereiden van leveren en afhalingen, enz.

De mogelijkheden zijn gigantisch, de evolutie razendsnel maar de risico's nemen in een even snel tempo toe. De risico's kunnen zich situeren op verschillende niveaus: een materieel-technisch gebrek in een toestel of apparaat maakt dat de verwerking niet of niet meer foutloos gebeurt. Bepaalde programmatie bevat kleine foutjes die niet opgemerkt zijn bij het testen en zich maar in uitzonderlijke gevallen manifesteren maar kunnen aanleiding geven tot gigantische problemen.

Een ander groot probleem en risico is dat men verschillende systemen en programmatie met elkaar laat praten en samenwerken. Niet alleen één op één, wat toch regelmatig reeds problematisch is maar in netwerken wat de complexiteit alleen maar verhoogt.

Verder is daar het aspect menselijke fout: door handelen of niet-handelen wordt schade aangebracht die leidt tot problemen.[1]

Tot slot dient men ook rekening te houden met opzet, bewuste nalatigheid en criminaliteit. Dit kan gaan om eigen mensen, eigen personeel of medewerkers die bewust schade wensen toe te brengen evenals mensen vreemd aan het bedrijf of de instelling die om allerlei motieven (persoonlijke zoals wraak, hebzucht, of motieven van organisaties zoals politieke of religieuze, terroristische) die verbanden, bestanden beschadigen of vernietigen of dreigen dat te zullen doen. [2]

---

1. Specialisten stellen dat één van de grootste uitdagingen voor beheerders van automatische systemen er niet bestaat ze te bedienen maar te begrijpen hoe de systemen werken en met welke algoritmes ze rekening houden. Als er iets fout gaat, moet men kunnen inschatten wat en waarom er zich een bepaald probleem voordoet en hoe men hierop correct inpikt om te remediëren. De ervaring leert dat supervisors heel vaak wel logisch op problemen reageren maar door een verkeerde inschatting van de systemen de problemen niet oplost maar verergert en het geheel totaal buiten controle geraakt met gigantische schaden tot gevolg.
2. Zowel in de USA die toch een trendzetter is als in Europa wordt tegenwoordig cyber en cyber criminaliteit in de jaarlijkse opiniepeiling bij risk managers ingeschat als het twee grootste risico dat hun ondernemingen bedreigt.

Belangrijk is zich bewust te zijn van de risico's op dit gebied, de mogelijke preventie om te vermijden dat dit gebeurt en de maatregelen om de gevolgen te beperken of financieel draagbaar te houden.

III. De actoren in het havengebeuren

Mensen die niet vertrouwd zijn met de haven en logistiek, onderschatten de complexiteit en het aantal actoren die bijdragen tot het gesmeerd ontvangen van schepen, lossen en laden ervan, opslaan, bewerken, administratief verwerken en doorvervoeren van goederen en passagiers.

We geven slechts een beperkte opsomming:

Aan de zijde van de overheid:

De Loodsen met de bijhorende loodsboten die tijdig aan boord moeten komen van de inkomende schepen om bijstand en advies te geven opdat ze veilig en tijdig de haven kunnen binnenvaren

De overheidsdiensten die zorgen dat de diepgang en de signalisatie, beboeiing en bebakening adequaat is en beantwoordt aan wat in de boekwerken staat beschreven. De tijdige melding van problemen: weggeslagen boeien, een gezonken schip, een pollutie, enz.

Verder de scheepvaartbegeleiding, de scheepvaartpolitie, de douane, de FOD's die toezien op kwaliteit van levende organismen en voedsel. Omkaderend de (gemeentelijke) havenbedrijven die faciliteren: zorgen voor de dokken, de waterwegen, kaaimuren en concessies, wegen, nutsvoorzieningen, sluizen en bruggen, enz.

Daarnaast ook talloze privé-bedrijven :

De dokloodsen, de shoregangers, de scheepsagenten met hun waterklerken, de expediteurs, de natiebedrijven, de stuwadoors, de expediteurs, de rederijen en andere vervoerders (binnenvaart, luchtvaart, spoor-& baanvervoer).

We maken een onderscheid tussen de de overheidsbedrijven en de privé-bedrijven omdat ze wegens het verschillend juridisch kader andere

verantwoordelijkheden hebben en op een andere manier deze kunnen inperken of uitsluiten. [1]

IV. Wat zijn de specifieke risico's verbonden aan cyber in havens, terminals, transport en logistiek ?

Het is onmogelijk in dit korte bestek een volledig overzicht te geven van wat we ons aan risico's kunnen voorstellen (risico's die zich intussen reeds hebben voorgedaan of die reëel zijn en waar men moet op anticiperen).

Om een zekere systematiek te houden in ons betoog, bespreken we de risico's aan de hand van de verschillende actoren in de haven en volgens de logistieke ketting. Men zal zien dat het fundamenteel telkens opnieuw draait om bestanden, data en het exploiteren van deze bestanden met het oog op beheer of doen werken van installaties of toestellen.

Een schip meldt aan dat ze een haven wenst aan te lopen. Om dat veilig te kunnen doen, moeten schepen natuurlijk perfect bestuurbaar zijn d.w.z. dat haar systemen werken: de motor functioneert normaal en is betrouwbaar, het roer, de schroeven, er kan versneld of vertraagd worden zo nodig en correct gemaneuvreerd, de communicatiemiddelen zoals radio en AIS (automatic identification system) zijn ingeschakeld en functioneren evenals de radar. De vereiste kaarten zijn aan boord evenals de info over de aanloop naar de haven en de haven zelf.

Scheepsbewegingscontrolediensten (meestal van de overheid) hebben dit schip reeds ruim vooraf gevolgd en ge-"earmarked", ze zien of het een correcte koers en snelheid vaart, binnen de voorzien lanes en aanlooproutes blijft, of er risico is op aanvaring, contact met een vast object of stranding.

---

1. We ondergaan echter de "Amerikanisering" van de samenleving waar er een "zero tolerance" heerst op het gebied van fouten en schaden onverbiddelijk leiden tot het zoeken van verantwoordelijke partijen die hiervoor moeten opdraaien, vaak met gigantische schadevergoedingen tot gevolg en "examplary fines and penalties" daar bovenop.

Dit lijkt allemaal logisch en eenvoudig echter dit dient ook te werken bij nacht en ontij en als de wet van Murphy toeslaat, kunnen de gevolgen gigantisch zijn.

Onze elektronische devices zijn zo makkelijk, zo adequaat en zo aanwezig dat we ons amper kunnen voorstellen hoe blind we opeens zijn als ze er niet zijn of niet betrouwbaar blijven (denk maar aan de situatie dat je een bestemming zoekt in een vreemde stad en je GPS valt uit).

Indien we het bovenstaande vanuit "cyber" analyseren, kunnen we te maken hebben met volgende problemen (en de opsomming is zeker niet exhaustief) :

De AIS van het schip valt uit (of is opzettelijk uitgezet of werd gemanipuleerd), de controledienst is dan reeds niet meer zeker of het schip wel het schip is dat werd aangekondigd. Is de lading wel deze die verwacht wordt ?

De radar van het schip functioneert niet naar behoren of er zijn problemen met de elektronische kaarten. We kunnen alleen maar hopen dat het schip over een tweede radar beschikt die wel functioneert en bijgewerkte hard copy kaarten aan boord heeft. Zelfs indien dit niet het geval zou zijn varen we niet noodzakelijk letterlijk af op een probleem maar dan valt men terug op vakkennis: kan de bemanning nog op een klassieke manier zonder GPS een correcte positie bepalen ? Een exacte positie op volle zee is niet absoluut noodzakelijk maar op een rivier vol zandbanken heeft men geen speling van enkele mijlen en moet men precies weten waar men zit.

Is de loods intussen reeds aan boord (ook het moederloodsschip mag niet blind zijn en weten waar het zich bevindt, waar en wanneer welke schepen kunnen verwacht worden die de haven dienen te worden binnengebracht), wordt het risico op problemen reeds sterk verminderd maar ook hij verwacht aan boord te komen van een goed functionerend schip met een professionele bemanning. [1]

---

1. De praktijk leert dat de kwaliteit van schepen en bemanning zeker van bepaalde jongere landen soms teleurstellend slecht is: schepen die niet kunnen achteruit varen, bemanning die het Engels niet beheersen en de meest elementaire werking van hun schepen niet kennen.

Zijn er effectief problemen, kan hij proberen zich te behelpen met radio-contact en zijn ervaring.

Er dient op gewezen te worden dat de problemen zich niet noodzakelijk aan de zijde van het schip situeren maar er kunnen bij voorbeeld ook problemen zijn met de radarketen langs de rivier.

Intussen heeft ons schip zich aangemeld om de sluis binnen te varen: ook hier kan men zich voorstellen dat er problemen zijn bij het versassen. Communicatie tussen de controletoren en de sluis, met de schepen in de sluis, met de sleepboten Het correct openen en sluiten van de sluisdeuren.

Ons schip wordt uiteindelijk door de sleepboten en dokloodsen veilig tegen de kade op de juiste ligplaats gebracht.

De waterklerk, politie en douane komen aan boord, papieren worden gecontroleerd. (Of de elektronische documenten: de cognossementen).

Er kan een aanvang worden gemaakt aan het lossen en laden van het schip. Afhankelijk van het type schip kan dit betekenen dat containers worden gelost en geladen, bij general cargo dat men weet wat waar staat en wat moet gelost worden en wat niet. In geval van lading van goederen, wat op de kade waar aan boord moet worden geplaatst. Telkens opnieuw dient te worden rekening gehouden met gewicht, stabiliteit, andere lading, volgende los- & laadhaven. In geval van vloeistoffen die gelost worden in landtank of overgepompt in andere schepen of binnenschepen dienen eveneens strikte veiligheidsprocedures gevolgd te worden. Natuurlijk dient men exact te weten wat zich waar bevindt, de specificiteiten van de lading volgens een Data sheet van de producent of opdrachtgever, juiste connectie, correcte lading en juiste hoeveelheid in de juiste tank.

Eens de goederen (meer en meer containers en meer en meer automatisatie en gigantische schaalvergroting[1]) gelost en in ontvangst

---

1. Singapore verplaatst haar containerhaven van het centrum naar het zuidwesten en wil daar tegen 2027 een volautomatische containerterminal bouwen met een capaciteit van 65 miljoen TEU. Dit is hallucinant in vergelijking met Antwerpen die momenteel 9 miljoen TEU kan behandelen. HERMANS, PH., "DEME wordt maritieme aannemer", *De Tijd*, woensdag 4 mei 2016, 19.

genomen zijn door de terminal [1] , is daar inherent een activiteit va bewaarneming aan verbonden. [2] Dit betekent dat goederen moete gecontroleerd worden op schade, de nodige reserves genomen worden, i stock genomen worden en terug uitgeleverd worden volgens d instructies van de klant. Eén mogelijkheid is dat de terminal zelf voor h transport tot op eindbestemming zorgt of dat een vervoerder aangedui door de klant/koper de goederen komt afhalen. Dit betekent dat d terminal perfect moeten waar de goederen staan, ze tijdig moeten kunne ter beschikking stellen van de klant voor belading of dit zelf organiseer In het kader van de opslag/bewaarneming vragen klanten of bieden d terminals die zich meer en meer als value added logistics bedrijve profileren allerlei bijkomende diensten aan zoals dedouanering, fiscal vertegenwoordiging, actief stockbeheer die rekening houdt me optimalisatie van de stockposities, het zo weinig mogelijk aanbreken va volledige palletten, het herverpakken van grote dozen naar detailhande etiketteren, assembleren, toevoegen van handleidingen, bewaken va vervaldagen, mengen, blenden, enz.

---

1. Een gigantische branchevervaging grijpt plaats in de haven en de logistiek in h algemeen. Voorheen waren stuwadoor en natiebedrijf aparte beroepen m duidelijk afgelijnde taken en aansprakelijkheden. Tegenwoordig streven rederije ernaar de volledige logistieke ketting van oorsprong tot eindbestemming t beheersen door die in eigen beheer te nemen en niet langer afhankelijk te zijn va lokale onafhankelijke partners. Stuwadoors nemen de activiteiten van natiebedri erbij evenals die van (multimodale) vervoerder. Baanvervoerders worde logistieke dienstverleners. Scheepsagenten worden vervoerders, enz. Dez branchevervaging is ook juridisch een buitengewone uitdaging om ee noodzakelijke maar aanvaardbare verdediging op te bouwen tegen claimanten di exorbitante claims kunnen indienen die het voortbestaan van deze bedrijven in h gedrang kunnen brengen.
2. Het oude gebruik in de Antwerpse haven dat goederen zich op risico van d eigenaar in opslag bevinden, wordt door de implementatie van ISPS en d afgesloten terminals die daar o.a. voor Antwerpen die steeds een "open haven was, almaar moeilijker te verdedigen. Dit in combinatie met het feit dat niet Europese opdrachtgevers met deze gebruiken niet vertrouwd zijn, dergelijke rege onbillijk vinden en er rechtbanken buiten Antwerpen bevoegd kunnen zij vermits zo bepaald in logistieke contracten, die deze gebruiken evenmin kenne en terzijde stellen.

De logistieke dienstverlener waakt over het respecteren van de invoerreglementering, fiscale wetgeving: invoerrechten, douane, accijnzen, BTW, voedselveiligheid, enz. Het illustreert duidelijk dat wat vroeger allemaal aparte beroepen of activiteiten waren zoals de stuwadoor, de natie, de expediteur, de scheepsagent, de douaneagent, de rivierbevrachter, de binnenvaartonderneming, het spoorwegbedrijf, de baanvervoerder, de commissionair-transporteur, de luchtvervoerder, het koerierbedrijf, de multimodale vervoerder, de NVOCC nu in het kader van de branchevervaging door één bedrijf worden aangeboden.

Of deze activiteiten nu worden uitgeoefend door verschillende partijen of door één of meerdere spelers die optreden in verschillende hoedanigheden, het illustreert de complexiteit van de informatiestromen, het internationaal karakter ervan en het belang van data, de juistheid, betrouwbaarheid en de snelle en permanente beschikbaarheid ervan.

Hier komen we tot het hart van de problematiek: Alle spelers in de ketting moeten zorgen voor het tijdig aanleveren en bijhouden van correcte data voor zichzelf, hun klant en de andere spelers in de ketting. Gaat hiermee iets fout dan kan dit de basis zijn voor gigantische problemen die afhankelijk van het juridisch vangnet kunnen leiden tot enorme schaden en evenredige claims.

V. Mogelijke preventiemaatregelen

De grootte van de verschillende spelers in de logistieke ketting voor het beheer van goederenstromen kan zeer verschillend zijn. Dit kan haar gevolgen hebben op het niveau van de aard en kwaliteit van de systemen waarmee data worden beheerd [1]. Ook de interne organisatie kan zijn invloed hebben: Is het bedrijf voldoende groot om een eigen insurance of risk-manager te hebben? Wie is verantwoordelijk voor cyber en de inherente risico's? : het hoofd van de IT afdeling ? Is ook de verantwoordelijke voor het operationele betrokken? De juridische dienst

---

1. Gaat het om intern ontwikkelde systemen of standaard software? Worden de systemen met eigen personeel ontwikkeld, tailor made, hoe up to date gehouden en aangepast aan nieuwe vereisten? Wat als er outsourcing is naar externe bedrijven?

of schadeafdeling? Of is dit een verantwoordelijkheid die word opgenomen op het niveau van de raad van bestuur? [1]

VI. Aansprakelijkheden van de verschillende actoren

We kunnen in deze paper onmogelijk de aansprakelijkheden van àll actoren onderzoeken maar zullen dit toch proberen voor enkel belangrijke dienstverleners en voor enkele representatieve bedrijven. W doen dit aan de hand van wat te vinden is op hun website.

Het Havenbedrijf Gent (HG) [2]

Het havenbedrijf Gent [3] heeft conform het havendecreet art. 2, 2° volgend taken

- *Het beheer en de exploitatie van het openbare en het private havendomein.*
- *De vastlegging en inning van de havengelden.*
- *De verlening van de havengebonden diensten (alle openbare dienstverplichtinge van het havenbedrijf die rechtstreeks of onrechtstreeks de overslag- e transportactiviteiten in het havengebied ondersteunen) aan de havengebruiker evenals de regeling en de vaststelling van de gebruiksvoorwaarden ervan.*
- *De uitoefening van de bijzondere administratieve politie.*

---

1. Sarah Stephens, partner – head of cyber, technology and Media E & O at JL Specialty, stressed that cyber risk is not just about data, but about automation reliance on technology and in effect, the transformation of the business. Cyber i not an IT issue. From the perspective of a chief information security officer, cybe means guarding against threats that come through the internet and are maliciou threats, but from insurance perspective we also mean lost laptops. There is disconnection there." Uit DOWDING, T., Cyber insurance – understanding th risk and coverage, *Commercial Risk Europe,* Volume 7, March 2016, 12.
2. www.havengent.be: We vinden op de site geen andere reglementen dan he tariefreglement die bepalingen bevatten met betrekking tot de wederzijdse rechte en plichten van de Haven Gent en haar gebruikers . Tariefreglement 2016 editi 2016/2 dd 4/2/2016.
3. Havendecreet: http://codex.vlaanderen.be/Zoeken/Document.aspx?DID=1006592&param=inhou d&ref=search

Wat zijn echter de aansprakelijkheden als HG er niet in slaagt deze taken naar behoren te vervullen en schade toebrengt aan gebruikers en derden ? Traditionaal gaat men ervan uit dat een overheidsbedrijf geen aansprakelijkheid heeft en enkel een inspanningsverbintenis heeft. Indien het fout gaat, roept ze overmacht in. Het tariefreglement bevat inderdaad vnl. plichten en verantwoordelijkheden van gebruikers. Enkel in art. 54 wordt er iets bepaald over de aansprakelijkheid van het HG zelf [1]

We weten niet welke situatie het HG precies viseert: Hoewel ze niet de effectieve uitbater is van concessies of terminals, probeert ze zich voornamelijk in te dekken tegen de gevallen van schade, verlies en diefstal van goederen, werktuigen en gebouwen (viseert men stadsmagazijnen ?). Daarvoor eist ze van de gebruikers dat ze een all-riskverzekering zouden afsluiten. Door het enkele feit van het deponeren van goederen op het havendomein is het HG vrijgesteld van elke aansprakelijkheid ten opzichte van gebruikers van de haven en van derden die in de plaats treden van deze gebruikers.

---

1. Artikel 54 ALGEMENE VOORWAARDEN c) Het Havenbedrijf kan geenszins aansprakelijk worden gesteld voor schade, verlies of diefstal.
Het stelt het havendomein ter beschikking in de toestand waarin het zich bevindt en kan niet aansprakelijk worden gesteld voor om het even welke schade, zelfs niet ingeval die te wijten is aan gebreken of aan onvoldoende onderhoud van het havendomein.
De havengebruikers moeten zelf op eigen kosten en verantwoording een allriskverzekering afsluiten voor de gebouwen, goederen, werktuigen en alle andere voorwerpen die door hun toedoen of door toedoen van hun opdrachtgevers zijn opgericht of op havendomein zijn gedeponeerd.
Alleen al door het feit dat de havengebruikers op havendomein goederen deponeren of opslaan, wordt het Havenbedrijf uitdrukkelijk vrijgesteld van elke aansprakelijkheid voor averij, verlies of schade die tengevolge van brand, ontploffing of enige andere oorzaak wordt aangericht aan havendomein en aan de gebouwen, goederen, werktuigen en voorwerpen die op havendomein zijn opgericht, zelfs ingeval er geen sprake is van toeval of overmacht. De voornoemde vrijstelling van aansprakelijkheid omvat ook de afstand van verhaal op alle personeelsleden van het Havenbedrijf. Deze vrijstelling van aansprakelijkheid omvat ook de afstand van verhaal bij indeplaatsstelling door derden in de rechten van het Havenbedrijf.

Het HG stelt echter elektronica ter beschikking van haar gebruikers bvb Enigma [1]. Gebruikers kunnen hiermee loodsen, sleepboten en andere diensten on-line reserveren. Verder verwerkt het scheepsgegevens, reis- en ladinggegevens. Verder is er GPS haven Gent, een applicatie die kan gedownload worden op de GPS van de gebruiker en dient om vlot de havennummers op de meest efficiënte manier te vinden. We vinden geen enkele bepaling qua aansprakelijkheid, limitatie over het gebruik van deze applicaties terug. Men kan zich echter wel de vraag wat de aansprakelijkheden als het niet werkt, foutief werkt of via een virus schade toebrengt aan de GPS van de gebruiker ?

Het Gemeentelijk Havenbedrijf Antwerpen (GHA) [2]

Op de website zijn onder de hoofding "verordeningen" allerhande reglementen en tarieven te vinden. De meest algemene zijn de "Havenonderrichting HKD 2015" en de "Gemeentelijke Havenpolitieverordening 2015, beiden van 8/1/2015. Ze bevatten echter geen beschrijving van de verantwoordelijkheden van het gemeentelijk Havenbedrijf.

In de meer specifieke verordeningen bvb de "Verordening op het gebruik van de wal-en mobiele havenkranen van het havenbedrijf Antwerpen" worden wel de aansprakelijkheden van het Havenbedrijf beschreven en zoveel mogelijk geëxonereerd.

Het GHA heeft een eigen IT-bedrijf AMARIS genaamd (Antwerpse Maritieme Infomatiesystemen). Volgens de site "ontwikkelt, implementeert en ondersteunt specifieke maritieme en aanverwante toepassingen en beheert tevens het computerpark van het GHA".[3]

---

1. www.enigmagent.com
2. www.portofantwerp.com
3. www.portofantwerp.com/nl/amaris#sthash.9ASyW9yl.dpuf Voor een haven is telematica een strategisch wapen. In de zeer competitieve maritieme wereld speelt IT een voorname rol in tal van bedrijfskritische aspecten: een vlot en veilig scheepvaartverkeer, de snelheid van behandeling, een strikte opvolging van (gevaarlijke) goederen, een efficiënt resources management voor personeel, materieel en gronden, en de correctheid van de financiële afwikkeling. Op al deze terreinen levert AMARIS performante, innovatieve en duurzame oplossingen. Voor elk project verdiept het zich in het specifieke business domein om met

Uit de website van het GHA kunnen we niet opmaken of en in welke mate het aansprakelijkheden accepteert of zich daarvoor probeert te exonereren. Eén ding is zeker het GHA is actief in het beheren en ontwikkelen van eigen programmatie en systemen die ze ter beschikking stelt van haar stakeholders en soms zelfs voor hen ontwerpt en verkoopt. Het bevestigt onze stelling van grote verbondenheid tussen verschillende netwerken en programmaties en het feit dat ook op dit niveau risico's gelopen worden qua cyber.

De Haven van Zeebrugge (Bestuur/MBZ nv) [1]

De website van de haven van Zeebrugge is in eerste instantie een commerciële website maar met goed te speuren, vonden we toch nog de havenverordening van [2] 28/1/1937. In de goede stijl van toen bepaalt art 91:

" De maatschappij wijst alle verantwoordelijkheid af voor enig ongeval dat aan personen en goederen binnen het beluik harer instellingen zou overkomen. Personen die zich om eenige reden binnen dit beluik bevinden en verblijven of er zich verplaatsen, doen zulks op eigen verantwoording."

Vermits men de moeite neemt om deze verordening op de site te vermelden, vermoeden we dat ze nog steeds toepasselijk en dat de MBZ nog steeds meent en hoopt hiermee haar vorderingen en verantwoordelijkheden te kunnen ontlopen. Het is echter duidelijk dat dit reglement op geen enkele wijze gedacht heeft aan mogelijke aansprakelijkheden wegens het niet, foutief functioneren van cybernetica.

---

aangepaste technologie de informatie- en communicatiebehoeften van de betrokkenen te kunnen lenigen. Vandaag beschikken de gebruikers van het Havenbedrijf over tientallen softwareapplicaties. Dit zijn zowel van derden aangekochte toepassingen die na marktonderzoek bleken tegemoet te komen aan de vooropgestelde eisen van onze gebruikers, als door AMARIS in huis gemaakte unieke toepassingen. Ook voor havengebruikers ontwikkelde AMARIS nuttige softwareapplicaties, zoals APICS2.

1. www.portofzeebrugge.be
2. Havenverordening Zeebrugge bekrachtigd bij KB dd. 28/1/1937. http://www.portofzeebrugge.be/sites/all/files/Verordening%20nederlands%201937_e-mailversie_0.pdf

De Haven van Brussel [1]

De website is eveneens een commerciële website. Een stuk ervan is voorzien voor professionelen maar geeft enkel contacten en technische gegevens. Onder rubriek documenten vinden we een tariefreglement [2]. In dat document wordt verwezen naar een reglement van 1/4/2006 dat we echter niet vonden.

In het tariefreglement worden enkel prijzen voor de concessies vermeld maar niets bepaald met betrekking tot de eventuele aansprakelijkheid van het havenbedrijf.

De *Port autonome de Liège* [3]

Op deze goed gemaakte website die beschikbaar is in vier talen is er een rubriek "onze voorwaarden". Deze worden echter niet vermeld op de site maar er worden de coördinaten opgegeven van twee personen die kunnen helpen om akkoorden op maat uit te werken.

Het loodswezen, maritieme dienstverlening en kust (MDK)[4]

De websites van de diverse instanties verwijzen naar reglementen, wetten en decreten maar vermelden niets inzake aansprakelijkheid. Het leerstuk van de immuniteit van de loods die slechts een adviserende functie heeft terwijl de kapitein meester blijft van zijn schip, zijn bekend. Ook het feit dat gewijzigde rechtspraak toch een aansprakelijkheid van de Staat en van de loods te persoonlijken titel kan opleggen in gevallen van grove schuld of grove nalatigheid. Dit viseert echter de situaties waar de loods het schip beloodst. Voor zover bekend is er geen rechtspraak voor de gevallen het loodswezen in gebreke blijft oa op het gebied van IT en cyber.

---

1. www.portdebruxelles.be
2. http://www.port.brussels/sites/default/files/documents/tariefreglement.pdf
3. www.portdeliege.be
4. www.loodswezen.be, www.agentschapmdk.be

VII. Het juridisch vangnet

Verzekeringsoplossingen

De cyberverzekering [1] is een vrij recent verzekeringsproduct dat haar oorsprong vindt in de Amerikaanse markt en er intussen een tiental jaren wordt aangeboden.

In Europa is het echter nog niet zo ingeburgerd maar de interesse ervoor neemt snel toe. [2] Volgens de verzekeraars is er voldoende capaciteit in de markt en zijn er adequate dekkingen te vinden die beantwoorden aan de specifieke noden en activiteiten van de klanten. Vraag is echter of de

---

1. De huidige producten die op de markt worden aangeboden zijn meer dan een aansprakelijkheidsdekking en zijn niet te verwarren met een computer All Risks of All Risks electronica verzekering (die in eerste instantie de vergoeding van schade aan of verlies van hardware beoogt) maar een hybride polis die enerzijds schade aan derden ten gevolge van het falen van datasystemen beoogt maar ook eigen schade. Het is dus maw meer dan een gewone ansprakelijkheidsverzekering. Het dekt ook meer dan schade of verlies veroorzaakt door criminelen extern of intern. Daarnaast bevat het ook een luik bijstand en assistentie dat misschien in geval van problemen voor de kleinere ondernemingen nog het meest waardevolle kan zijn.
2. In die zin wordt verwacht dat de cyber verzekering een evolutie zal meemaken zoals destijds de D&O polis (bestuurdersaansprakelijkheid) waar het in eerste instantie een polis was die enkel onderschreven en betaald kon worden door zeer grote beursgenoteerde bedrijven en nu zelfs behoort tot de corporate governance van een VZW. Het verschil in ontwikkelingssnelheid van de cyberpolis tussen de USA en Europa heeft o.a. te maken met het feit dat in de USA reeds wetgeving bestaat die de beheerder van data verplicht om de betrokkenen en de overheid te verwittigen van een lek in de data. Een gelijkaardige wetgeving (de General Data Protection Regulation GDPR) is einde 2015 ook op Europees niveau goedgekeurd en wordt van kracht in 2018. Naast de mededelingsplicht waarvan de kosten bvb voor een bank, een verzekeringsmaatschappij of een supermarkt wegens hun groot aantal klanten gigantisch kunnen oplopen, kan de overheid daarenboven boetes opleggen die tot 4% van de omzet bedragen. De underwriter van Beazley en AIG bevestigen dat de interesse van CAC40 bedrijven snel toeneemt en verwacht dat ze allemaal tegen einde 2016 een cyber polis zullen onderschreven hebben. Ook tekent de trend zich af om hogere limieten te onderschrijven. NORRIS, B. & COLLINS, S., Market battles hard for cyber as data protection rules shift landscape , *Commercial Risk Europe,* Volume 7, March 2016, 10.

dekkingen zullen aangeboden worden aan een prijs die de potentiële klanten bereid zijn om te betalen.

Vermits in cyber alles onderling verbonden is, dienen verzekeraars ernstig rekening te houden met het risico op accumulatie van schaden bij één gebeurtenis. Dit is echter moeilijker dan het lijkt. Geïsoleerde en specifieke cyber polissen kan men nog in kaart brengen maar er kan ook een stuk cyber dekking zitten in een property of aansprakelijkheidspolis.

Men verwacht niet dat een toenemende vraag de premies zullen doen misschien net zoals bij D&O integendeel. Het product en de risico's zijn echter niet vergelijkbaar cf. o.a. het grotere accumulatierisico. Specialisten zijn het over eens dat momenteel de prijsstelling voor cyber in Europa eerder goedkoop is. De wetswijziging die eraan komt, zware schaden in de USA kunnen echter wel invloed hebben en verzekeraars er toe aanzetten streng te selecteren bij hun acceptatie en enkel competitief te zijn voor bedrijven die hun cyber risico's zo goed als mogelijk onder controle hebben.

Sommige risk-managers menen dat de aangeboden producten geen volledige oplossing zijn voor hun noden. Dat is inderdaad gedeeltelijk waar maar tegenwoordig bevat een cyber polis naast first en third party aansprakelijkheid, ook business interruption en crisismanagement.

"Houston, we have a problem ? ": een cyber probleem, wat nu ?

VIII. Besluit - Aanbevelingen

Cyber is meer aanwezig dan men op het eerste zicht kan vermoeden en is veel meer dan een IT aangelegenheid.

Het is om die reden ook niet de exclusieve verantwoordelijkheid van een IT manager maar van de raad van bestuur en per definitie multi-disciplinair. IT inderdaad maar ook het operationele, het juridische en sales moeten er eveneens bij betrokken worden.

Het zou een vergissing zijn te denken dat malware, cyber-attack extern of intern enkel bij de buren gebeurt. Door de internationalisering en de verstrengeling van systemen, internet en automatisering van machines, kan een aantasting van overal komen.

Om die reden is een business continuity plan (BCP) een minimum vereiste van corporate governance.

Dit moet echter continu worden bijgestuurd en getest en getoetst in de mate van het mogelijke.

Verder is het moeilijk om deze problematiek enkel te proberen te beheersen binnen het eigen bedrijf. Niets belet mits goede afspraken af te stemmen en lessons learned uit te wisselen met sector genoten of bedrijven met een gelijkaardige problematiek. Er zijn ook mogelijkheden via de beroepsorganisaties.

Vermits we zagen dat in geval van probleem de financiële gevolgen van eigen schade en schade aan derden zeer groot kunnen, zijn verdient het aanbeveling waar nodig en mogelijk een juridisch vangnet uit te bouwen via algemene voorwaarden of specifieke clausules in logistieke tailormade contracten. Voor de extra-contractuele aansprakelijkheid en voor aansprakelijkheden die paramount worden opgelegd door de overheid is dit echter geen oplossing en rest enkel de mogelijkheid van het afwentelen van het risico op verzekeraars. Bepaalde risico's kunnen reeds gedekt zijn door de klassieke bestaande polissen voor andere zal men moeten onderzoeken of een zgn. cyber-polis een oplossing kan bieden. Lacunes en dubbele dekkingen zal men zo goed als mogelijk moeten in kaart brengen. Ook de keuze van de adequate limieten zijn niet eenvoudig

Bibliografie

Oxford dictionary: definitie van cyber:
http://www.oxforddictionaries.com/definition/english/cyber

Commercial Risk Europe: vakmagazine voor verzekeringen en risk management : www.commercialriskeurope.com Dit magazine verschijnt wekelijks in hard copy en elektronisch.

Vlaams Instituut voor de Logistiek: www.vil.be cfr de projecten en nieuwsbrieven inzake gebruik van innovaties zoals drones, RFID-tags, cobots in logistics (collaborative robots die bvb samen kunnen werken met mensen bij taken zoals verpakken en sorteren en op die manier het rendement en efficiëntie verhogen.

SCHNEIDER, L., Cyber-risques & cyber-assurances, http://docplayer.fr/2008446-Banque-strategie-enass-papers-9-cahier-de-prospective-bancaire-financiere-dossier.html

STEPHENS, S. & FORT, S., Cyber Liability & Higher Education, Aon Professional Risk Solutions White paper, December 2008, http://www.aon.com/about-aon/intellectual-capital/attachments/risk-services/cyber_liability_higher_education.pdf

Enigma systeem Haven Gent: www.enigmagent.com

* *
*