

## Sicherheit im Containerverkehr

**Dr. Frank Arendt**

*Institut für Seeverkehrswirtschaft und Logistik (ISL)*

*Direktor Abteilung Informationslogistik*

*Universitätsallee GW 1 Block A, 28539 Bremen*

*phone: +49-421-22096-17, fax: +49-421-22096-55, e-mail: arendt@isl.org*

***Dieser Beitrag ist zur Veröffentlichung vorgesehen im Jahrbuch 2006 der Hafentechnischen Gesellschaft e.V. "Logistik", mit freundlicher Genehmigung der HTG***

### **1 Hintergrund**

Seit Anbeginn des Gütertransports spielte das Thema Sicherheit von Ladung und Transportmitteln eine wichtige Rolle. Unter Sicherheit sei hier verstanden, dass das Transportgut, das Transportmittel und auch betroffene Personen ohne Schaden am Bestimmungsort ankommen und alle Risiken auf diesem Weg möglichst ausgeschaltet werden. Im englischen Sprachgebrauch findet man zwei Ausprägungen für den deutschen Begriff Sicherheit, und zwar „Safety“ und „Security“. Safety bezeichnet die Sicherheit vor Umwelteinflüssen und unvorhergesehenen Ereignissen (z.B. Sturm, Ausfall einer Ruderanlage, menschliches Fehlverhalten), während Security die Sicherung vor mutwilligen kriminellen Aktionen bezeichnet. Diese Sicherheitsaspekte können einander unter Umständen ausschließen. Ein versperrter Eingang zur Vermeidung des unbefugten Zutritts, etwa im Container-Terminal - könnte als versperrter Ausgang im Notfall verheerende Folgen haben.

Dieser Beitrag wird sich mit dem zweiten Aspekt – bezogen auf den Containerverkehr mit seinen Charakteristika der weltweiten Standardisierung und intermodalen Eignung - beschäftigen.

Bereits seit fast 7000 Jahren (!) beschäftigt man sich mit dem Thema Ladungssicherung, um zu gewährleisten, dass der Inhalt eines Ladungsträgers während des Transports nicht verändert wird. Tonbehälter wurden versiegelt und gestempelt – der Vorläufer heutiger Containersiegel. Abbildung 1 zeigt einen solchen versiegelten Behälter aus der Zeit von 5200 v. Chr.

**Abb. 1: Versiegelter „Container“ aus der Vorzeit (Nationalmuseum Damaskus)**



## **2 Risiken und Gefahren**

Die seit jeher diskutierten Transport bezogenen Risiken waren Schmuggel, Diebstahl, Piraterie, blinde Passagiere sowie die Fälschung von Frachtpapieren wie z.B. Manifesten. Seit dem 11. September 2001 ist der internationale Terrorismus als zuvor weitgehend unbeachtete neue Bedrohung hinzu gekommen. Diese Bedrohung gegen Personen, die Wirtschaft allgemein sowie die Regierungen umfasst, dass

- Schiffe (als hochwertige Assets) als Ziele von Angriffen in Frage kommen
- Schiffe als Waffe dienen können (Angriffe Schiff gegen Schiff bzw. Schiff gegen Infrastruktur, z.B. Hafenanlagen oder Brücken)
- Container als Waffe mit illegal transportierten Massenvernichtungswaffen eingesetzt werden könnten
- Container als Behausung für den Transport und die illegale Einwanderung von Terroristen missbraucht werden könnten.

Neben der Transport-Infrastruktur (Brücken, Tunnel, Umschlagseinrichtungen, Gleise, Schleusen) scheinen Ladung und Fahrzeuge besonders angreifbar zu sein.

Das Bedrohungspotenzial kann als Kombination aus Angreifbarkeit und Auswirkungen klassifiziert werden. [DNV05] unterscheidet zwischen Infrastruktur-Risiken als Zerstörung von Infrastruktur-Elementen, um Transportketten und –netzwerke zu unterbrechen und damit einen hohen volkswirtschaftlichen Schaden anzurichten und Supply-Chain-Risiken als Missbrauch der Supply Chains, um Zerstörungen anzurichten. Hierbei sind Transportmittel nicht das Ziel, sondern das Hilfsmittel.

Dieselbe Quelle nennt geschätzte 6,6 Mrd. € Schaden, wenn ein europäischer Haupt-Transportkorridor unterbrochen wird sowie 200 bis 500 Mrd. € Schaden bei einer Nuklearexplosion in einer der großen Hafenstädte.

Dass diese Gefahren nicht allein hypothetischer Natur sind, zeigen folgende Fälle:

- Der amerikanische Zerstörer „USS Cole“ wurde im Jahre 2000 im jemenitischen Hafen Aden beschädigt, als zwei Selbstmordattentäter der Al Kaïda ein mit Sprengstoff beladenes Schlauchboote an der Bordwand explodieren ließen. Es entstand ein großes Loch in der Außenwand (Abb. 2); 17 Besatzungsmitglieder starben; 38 wurden verletzt.

**Abb. 2: Attackiertes Schiff MSS Cole (Quelle: <http://www.lockport-ny.com/>)**



- Im Jahre 2002 wurde vor der Küste Jemens ein Anschlag auf den französischen Öltanker „Limburg“ verübt. Der mit 398.000 Barrel Rohöl beladene Doppelhüllen-Tanker wurde von einem kleinen Boot voller Sprengstoff gerammt (Abb. 3). Insgesamt zwölf Besatzungsmitglieder wurden verletzt.

**Abb. 3: Attackiertes Schiff Limburg (Quelle: <http://www.middle-east-online.com/>)**



### 3 Maßnahmen zur Eindämmung der Gefahren

Die o.g. Bedrohungen ließen verstärkte Sicherungsmaßnahmen entstehen, um diese, wenn auch nicht ganz auszuschließen, so zumindest vermindern zu können.

In der Folge der Al-Kaida-Angriffe auf New York und Washington wurden im wesentlichen durch die USA und hier speziell durch das neu gegründete „Department of Homeland Security“ (DHS, Heimatschutzbehörde) initiierte Maßnahmen ergriffen. Das DHS beinhaltet 22 verschiedene Organisationen und hat ca. 180.000 Mitarbeiter, es ist thematisch in fünf Aufgabengebiete unterteilt: Emergencies & Disasters, Travel & Transportation, Immigration & Borders, Research & Technology, and Threats & Protection. Ein wichtiger Bereich des DHS ist die Einheit Customs and Border Protection (CBP).

Der Containerverkehr bildet aus US-amerikanischer Sicht nicht umsonst einen starken Fokus in punkto Sicherheitsmaßnahmen: 95 % aller Güter werden in Containern in die USA eingeführt. Es gibt insgesamt etwa 150 Häfen in den USA, davon etwa 40 mit internationaler Bedeutung. Im Jahr 2003 fertigte der US Zoll ca. 9 Millionen Übersee-Container ab [ISL05].

Diese Maßnahmen zielen u.a. auf die Minimierung der Angreifbarkeit und die Minimierung der Auswirkungen, z.B. durch

- organisatorische und physische Sicherungsmaßnahmen entlang der Transportkette, z.B. für Häfen und Schiffe, zu verstärken (z.B. durch strikte Zugangskontrolle)
- Verdachtsfälle auf dem Vorwege zu überprüfen
- Hochsicherheitssiegel für den Türverschluss zur Pflicht zu machen.

Einige der in diesem Zusammenhang relevanten Verordnungen und Initiativen – neben der DHS von der International Maritime Organisation IMO (<http://www.imo.org/>) - sind im Folgenden aufgeführt:

#### 3.1 ISPS Code (International Ship and Port Facility Security Code)

Als Erweiterung der SOLAS-Convention (International Convention for the Safety of Life at Sea, 1974) wurde von der IMO der ISPS-Code geschaffen [IMO03]. Dieser Code befasst sich mit der Erhöhung der Sicherheit an Bord von Güterschiffen (> 500 BRZ) und in Hafenterminals. Zur Erfüllung dieses Codes (Zertifizierung) werden Gefahrenabwehrpläne der Betreiberfirmen (Umschlagsbetriebe, Reeder) erstellt und durch sog. „Designated Authorities“ (DAs), die von jedem Staat ernannt wurden, genehmigt. In Deutschland ist das Bundesamt für Seeschifffahrt und Hydrographie in Hamburg für die unter deutscher Flagge fahrenden Schiffe zuständig; für die Umsetzung bei den Umschlagsbetrieben ist dies z.B. für die bremischen Häfen der Senator für Wirtschaft und Häfen in Bremen.

Der ISPS-Code besteht aus einem Pflicht- und einem freiwilligen Teil; die Umsetzung der Vorschriften ist z.T. interpretationsfähig, so dass eine weltweite Vereinheitlichung nicht unbedingt gegeben ist. Die Zertifizierung musste am 01.07.2004 vorhanden sein, ansonsten drohten Benachteiligungen bei der Einfahrt oder der Abfertigung eines Schiffes. Es werden verschiedene 'neue' Rollen geschaffen (SSO - Ship Security Officer, CSO - Company Security Officer, PSO - Port Security Officer, PFSO – Port Facility Security Officer etc.) und entsprechende Ausbildungen und Übungen vorgeschrieben.

---

### 3.2 C-TPAT (Customs-Trade Partnership against Terrorism)

Diese ab 2002 gültige Initiative ist eine Partnerschaft zwischen der US-Zollbehörde und der US-Wirtschaft zur Bekämpfung des internationalen Terrorismus (im Internet zu finden unter [http://www.customs.ustreas.gov/xp/cgov/import/commercial\\_enforcement/ctpat/](http://www.customs.ustreas.gov/xp/cgov/import/commercial_enforcement/ctpat/)). Durch die freiwillig eingegangenen Verpflichtungen der Firmen soll für die Sicherheit der ganzen Versorgungskette bis hin zum Endverbraucher in den USA gesorgt werden.

An diesem Programm können sich Frachtführer, Spediteure und Importeure beteiligen. Dieses beinhaltet die Überprüfung des jeweiligen Unternehmens durch die US-Zollbehörde. Hieraus können Maßnahmen für die Firma resultieren, die Sicherheit zu erhöhen, welche auch durch die Zollbehörden überprüft werden können. Die vorgeschlagenen Maßnahmen können vielschichtig sein und reichen von Zugangskontrollen zum Betriebsgelände, sichere Verpackung und Versendung, sowie Sicherheitsüberprüfungen von Mitarbeitern. Vorteile bei der Partnerschaft sind schnellere und vereinfachte Abfertungsverfahren in den Seehäfen.

### 3.3 CSI (Container Security Initiative)

Der Bedrohung durch terroristischen Missbrauch der Containertransporte im weltweiten Seeverkehr soll die Container Security Initiative CSI (im Internet zu finden unter [http://www.customs.ustreas.gov/xp/cgov/import/cargo\\_control/csi/](http://www.customs.ustreas.gov/xp/cgov/import/cargo_control/csi/)) entgegen wirken. Die Ziele der CSI sind: Aufstellung von Sicherheitskriterien zur Identifizierung von Containern mit hohem Risiko basierend auf vorangegangenen Informationen, Anwendung von neuen Technologien zur Überprüfung von Risikocontainern, Entwicklung von sicheren und „smart“ Containern. Durch diese Initiative wird die Sicherheitskontrolle vom Transit- oder Löschhafen in den USA auf den Ladehafen außerhalb der USA verlagert und damit die sicherheitstechnische Außengrenze der USA quasi in die Abgangsländer verlagert. Es ist eine freiwillige Partnerschaft der nationalen Zollbehörden und der US-Zollbehörde (US Customs), bei der US-Zollbeamte, z.B. in den deutschen Abgangshäfen Bremerhaven und Hamburg, den deutschen Zöllnern beratend zur Seite stehen.

In der Praxis werden den US-Zollbeamten Einsicht in die EDV-Systeme des US-Zolls gegeben, um – in Absprache mit den lokalen Zollbehörden - risikobehaftete Container aufzuspüren, diese bereits im Abgangshafen zu durchleuchten und/oder zu öffnen und zu durchsuchen.

Das CSI-Abkommen beruht auf Gegenseitigkeit, wird jedoch z.B. von europäischen Zollverwaltungen in USA derzeit nicht umgesetzt.

### 3.4 24-Hour Rule

Die USA haben mit der '24-Hour Rule' ein weiteres Instrument der vorzeitigen Ablehnung der Einfuhr von Containern geschaffen und im Dezember 2002 verbindlich eingeführt (im Internet zu finden unter [http://www.customs.ustreas.gov/xp/cgov/import/carriers/24hour\\_rule/](http://www.customs.ustreas.gov/xp/cgov/import/carriers/24hour_rule/)). Spätestens 24 Stunden vor der Schiffsbeladung im Ladehafen muss das Manifest u.a. mit detaillierten Angaben zu Ladung, Fahrtroute, Verloader und Verladehafen des Containers bei der US-Zollbehörde eingegangen sein. Nachträgliche Änderungen an den Manifesten

---

werden nicht akzeptiert, möglicherweise wird das Laden des Containers oder die Transitmöglichkeit eines Containers untersagt.

### 3.5 Spezielle deutsche Maßnahmen

Neben der Umsetzung internationaler Vorschriften sind auf deutscher Ebene hauptsächlich zwei Einrichtungen zu nennen:

- Der Bund-Länder-Arbeitskreis Maritime Security (BLAMS) u.a. mit Vertretern des Bundes und der Behörden der Küstenländer. Hier wird über gemeinsame Vorgehensweisen und Umsetzung von internationalen Vorschriften in den Ländern diskutiert, um unterschiedliche Strukturen zu vermeiden.
- Vor kurzer Zeit wurde das maritime Sicherheitszentrum (MSZ) mit Havariekommando in Cuxhaven als zentrale Kontaktstelle unter Leitung des Bundesministeriums für Verkehr, Bau und Stadtentwicklung (BMVBS) eingerichtet, die alle sicherheitsrelevanten Meldungen über Schiffe, Häfen und Wasserstraßen innerhalb der Hoheitsgewässer bekommt und an zuständige Behörden und Organisationen weiterleiten soll. Diese Stelle ist als nationale Informationsdrehscheibe geplant, um Informationsdefizite zu vermeiden. Eine solche Organisation soll in jedem Staat existieren, der Schiffe, Hafeneinrichtungen und/oder Wasserstraßen, welche unter die entsprechenden Gesetze fallen, besitzt.

### 3.6 Sonstige Initiativen

Über die o.g. Maßnahmen gibt es noch eine Vielzahl weiterer Regularien, Initiativen und Feldtests, die hier (ohne Anspruch auf Vollständigkeit) kurz erwähnt werden sollen:

- **CHCP (Cargo Handling Cooperative Program)**  
Eigene Organisation mit den Zielsetzungen, Innovationen im Containerhandling zu fördern, durch Forschung und Entwicklung die Produktivität zu steigern, Sicherheitsaspekte im Containerhandling zu unterstützen sowie Trainings- und Fortbildungsmaßnahmen zu innovativen Themen durchzuführen. In diesem Rahmen wurden z.B. Tests mit RFID-Siegeln in den USA durchgeführt (<http://www.marad.dot.gov/Programs/CHCP/>).
- **CSC (International Convention for Safe Containers)**  
Diese im Jahre 1972 von der International Maritime Organisation (IMO) erlassene und inzwischen mehrfach modifizierte Konvention [IMO93] definiert einen Sicherheitsstandard für Containern, um einerseits das Risiko für am Transport beteiligte Personen zu minimieren und die Vereinheitlichung der Sicherheitsvorschriften für alle weltweiten Oberflächentransporte andererseits zur Vereinfachung des internationalen Transports. Mittel sind Richtlinien für Containertests, Stabilitätsvorschriften, Wartung und Inspektionen.

---

- **Trusted Shipper Program**

Eine weitere Komponente zur Verhinderung, dass gefährliche Container in Umlauf kommen, ist das Trusted Shipper Program, das Versender und Packbetriebe weltweit auf ihre Unbedenklichkeit überprüft. Diese Initiative wurde vom US Department of Customs and Border Protection initiiert und kommt ursprünglich aus dem Luftverkehr und hat enge Verbindungen zu C-TPAT.

- **OSC (Operation Safe Commerce)**

Hier wurden unter US-amerikanischer Initiative (Department of Transport und US-Zollbehörde) ab 2002 ausgewählte Container-Lieferketten aus Europa in die USA betrachtet, um diese pilothaft mit Hilfe elektronischer Siegel zu sichern. Container wurden mit RFID-Siegeln, Terminals mit Lesegeräten ausgestattet. Nach Beendigung der Tests wurde das Equipment wieder demontiert.

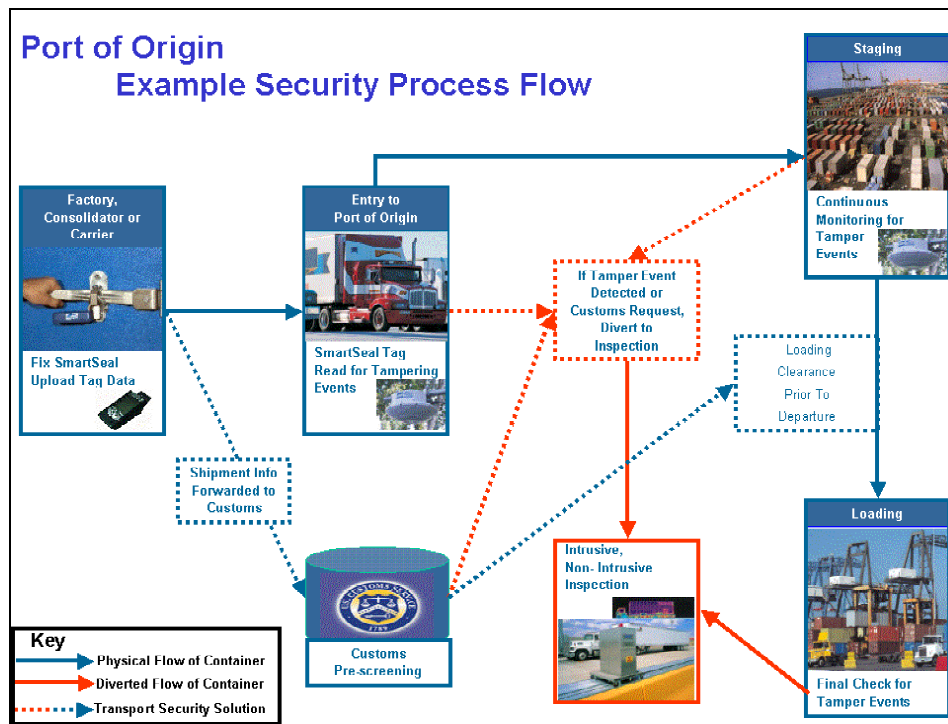
- **SST (Smart and Secure Tradelanes)**

Die Initiative SST ist vom Strategic Council on Security Technology (SCST) der USA gegründet worden (vgl. <http://www.scst.info/>). Es ist eine von der Industrie vorangetriebene Sicherheitsinitiative der Versorgungskette. Es soll die Sicherheit von Transporten zwischen dem Hersteller und dem Endverbraucher innerhalb aller weltweiten Handelsketten erhöhen.

Aufkommende technologische Trends, Geschäftsprozesse und Regierungspolitik werden im Zusammenhang mit der Sicherheit der Transportketten beobachtet. Studien, behördliche Berichte und Initiativen der Industrie werden gefördert, um die Gesamtheit der heutigen praktischen Sicherheit in den benannten Gebieten zu verstehen. Neue Erkenntnisse werden zu neuen Lösungen weiterentwickelt und als Informationsquelle der Transportgemeinschaft zur Verfügung gestellt. Erste Tests mit „Smart Containern“ haben bereits stattgefunden.<sup>13</sup> Häfen (z.B. Los Angeles, Hongkong, Rotterdam) haben ihre Terminals mit Empfangsantennen ausgerüstet; über 800 Container wurden einbezogen; in einer zweiten Phase sollte das Netz auch auf das Hinterland ausgeweitet werden [HOL03].

Ein exemplarischer Informationsfluss ist in Abb. 4 enthalten:

Abb. 4: SST Ablauf-Szenario [EVE03]



## 4 Technische Möglichkeiten

Spezielle technische Möglichkeiten der Sicherung des Container-Transports werden in letzter Zeit verstärkt diskutiert und erprobt. Doch neue Technologien können auch erhöhte Risiken mit sich bringen. Die Ausrüstung aller Seeschiffe mit AIS-Transpondern ermöglicht ihre permanente weltweite Positionsverfolgung. Frei zugängliche Dienste wie AIS-Live (<http://www.aislive.com/>) ermöglichen die Positionsabfrage für Jedermann – auch für Personen mit unlauteren Absichten.

Zwei Beispiele für viel versprechende Entwicklungen seien hier genannt.

### 4.1 Das Elektronische Siegel

Das E-Seal oder elektronische Siegel verbindet die Vorteile eines mechanischen Bolzensiegels mit einem Radio-Transponder (RFID). Die Daten des elektronischen Siegels (z.B. Siegelnummer und Status) können berührungslos ausgelesen werden und bringen so auch zusätzlichen Nutzen, z.B. bei der Siegel-Identifizierung im Seehafen. Die globale Ausrichtung des Containerverkehrs bringt allerdings die Notwendigkeit der weltweiten technischen Standardisierung dieser Siegel mit sich – ein Vorhaben, dem sich die ISO-Arbeitsgruppe TC 104 (Freight Containers) unter der Norm ISO 18185 gewidmet hat. Ein Standardisierungsentwurf wird im Winter 2005/2006 erwartet; noch scheint allerdings auch ein marktgetriebener Ansatz über große Container-Reedereien möglich.

Zum Dateninhalt der elektronischen Siegel gibt es prinzipiell zwei Ansätze: während der minimalistische nur Basisinformationen wie Siegelnummer und –zustand vorsieht, verfolgt

der komplette die Speicherung der gesamten Information über Container, Ladung und Route. Der erste Ansatz hat sich durchgesetzt, da das Sicherheitsrisiko (z.B. für Diebstähle) beim zweiten ungleich höher wäre.

Zurzeit werden Einwegsiegel favorisiert, da jegliche Wiederverwendung von Siegeln wie auch die Möglichkeit, Daten zusätzlich zu speichern, aus Sicherheitsgründen abgelehnt wird.

Technische Tests wurden u.a. in den USA im Rahmen des sog. Cargo Handling Co-Operative Program durchgeführt [CHCP04]; ein umfassendes Konzept für den Einsatz elektronischer Siegel einschließlich der Berücksichtigung der Interessen aller beteiligten Unternehmen und Behörden sowie der Diskussion einer zentralen Plattform für die sicherheitsrelevanten Daten wurde z.B. im Jahre 2004 im Projekt COSI (Container-Sicherheit) unter Förderung der Bremer Landesinitiative bremen in t.i.m.e. erarbeitet (Details unter <http://www.mobilecity.org>).

## 4.2 Smart Container

Diese Technologie setzt nicht nur auf die Türsicherung wie das elektronische Siegel, sondern bezieht zusätzliche Sensoren mit ein. So sind etwa Positionsbestimmung über GPS, Licht- und Türsensoren, Mayday-Funktionen sowie Sensoren zum Aufspüren von Personen oder Massenvernichtungswaffen möglich. Probleme bilden hier in erster Linie die Kosten für die Ausrüstung und Wartung.

Die permanente Positionsverfolgung von Containern scheint nur für solche mit hochwertiger oder besonders gefährdeter Ladung sinnvoll – allein aus Kostengründen. Für die Standard-Container ist in der Regel eine Statusverfolgung über Statusnachrichten (versiegelt, Beladungsort des Verladers mit Lkw verlassen, Gate-Eingang Terminal, Verlademeldung, Löschmeldung, etc.) ausreichend.

## 5 Wie geht es weiter?

Die bisher getroffenen Maßnahmen stellen einen ersten Schritt in Richtung „sichere Container-Transportkette“ dar. In den nächsten Monaten und Jahren werden diese Maßnahmen noch verschärft werden, wobei die Balance zwischen erhöhter Sicherheit und den damit verbundenen erhöhten Kosten bzw. dem freien Warenverkehr stets zu berücksichtigen sein wird. Man muss sich darüber im Klaren sein, dass das Aufhalten eines Schiffs mit 8000 oder mehr TEUs bzw. ein Einlaufverbot wegen eines potenziell gefährlichen Containers an Bord durch den dadurch entstehenden ökonomischen Schaden nur in gut begründeten Verdachtsfällen gerechtfertigt erscheint.

Die Risikoabschätzung fällt schwer: Als wie wahrscheinlich wird ein terroristischer Akt, der über Häfen vorbereitet wird, gesehen? Welche Vorkehrungen sind gerechtfertigt? Wo liegt die größte Schwachstelle im gesamten Prozessablauf? Ist „schmutziger Inhalt“ am Einfachsten bereits beim Packen des Containers einzubringen und kommt dann sicher versiegelt zum Zielort oder gestaltet sich dies während des Transports reibungsloser? Müssen auch als Leercontainer deklarierte Container (die evtl. gar nicht leer, aber gut zugänglich sind) zukünftig versiegelt werden? Welche Maßnahmen sollen Pflicht werden, welche auf freiwilliger Basis beruhen (und damit evtl. einen Wettbewerbsvorsprung bedeuten)? Viele Fragen, die in den nächsten Jahren zu beantworten sind.

---

Einige konkret erwartete zukünftige Maßnahmen sind:

- Seal Verification Program: Ab 2007 wird ein verschärftes Sicherheitsprogramm der USA im Containerverkehr erwartet. Ziel ist die Verpflichtung der Ladehäfen für US-Exportverkehre zur Einhaltung der Überprüfung von Containersiegeln speziell bei der Gate-Abfertigung der LKWs sowie bei Transitcontainern – also jenen, die per Schiff angeliefert und ausgeliefert werden.
- Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Verbesserung der Gefahrenabwehr in Häfen [EUR04] zur Ausweitung der o.g. Verordnung und damit des ISPS-Codes auf das gesamte Hafengebiet über die Terminals/Umschlagsanlagen hinaus.
- Entwicklung einer Richtlinie „Intermodal Freight Transport Security“ durch die Europäische Kommission. Der ISPS-Code zielt auf die Sicherung von Terminals und Schiffen. Ziel muss es sein, die gesamte Transportkette vom Beladen des Containers bis zum Öffnen durch den Empfänger in einer Weise zu sichern, bei der sich Sicherheit und Zusatz-Kosten in ein vernünftiges Verhältnis stehen. Diese Richtlinie „Intermodal Freight Transport Security“ wird voraussichtlich im Jahre 2006 verabschiedet werden; in ihr wird nicht nur auf Außengrenzen (wie bei den US-Vorschriften), sondern auch auf Verfahren innerhalb der EU abgezielt. Dieses Thema wird u.a. in [DNV05] detailliert aufgegriffen. Hier werden folgende Aussagen getroffen:
  - Bestehende Gesetzgebungen berücksichtigen nicht alle Verkehrsträger. Diese beschränkt sich hauptsächlich auf den Seeverkehr, Luftverkehr und auf Gefahrguttransporte per Straße, Schiene und Binnenschiff.
  - Die meisten EU-Mitgliedsstaaten haben noch keine übergeordnete Sicherheitspolitik.
  - Einige große Firmen haben eigene Sicherheitsmaßnahmen für ihre Supply Chains ergriffen. Für die kleineren trifft das nicht zu; zudem ist das Bewusstsein bzgl. terroristischer Gefahren eher schwach ausgeprägt.
  - Der EU-Ministerrat hat die Notwendigkeit des Schutzes von Transporten über Verkehrsträger hinweg auf dem Territorium der EU-25 definiert.

Die EU-Kommission zielt auf einen Rahmen für die Sicherung kompletter Lieferketten, der von den Mitgliedsstaaten umgesetzt werden muss. Hierbei handelt es sich – wie bei allen bisherigen Pflichtmaßnahmen auch – um regulatorische Maßnahmen. In [DNV05] werden zwei Phasen vorgeschlagen: eine freiwillige Phase von 2006 bis 2008 mit Anreizen für Teilnehmer (z.B. soll der Status als „Secure Operator“ verliehen werden und „Green Lanes“ für die bevorzugte Abfertigung von Teilnehmern eingerichtet werden) und eine Pflichtphase ab 2009 (mit Strafen bei Nicht-Erfüllung).

Dieselbe Quelle nennt als wesentliche Maßnahmen u.a. sog. „Audit Schemes“ (mit geschätzten 6000 bis 7000 Auditors) und „Enforcement Schemes“ zur Zertifizierung von Beteiligten entlang der Kette. Ferner wird neben der Betonung der Bedeutung von Containersiegeln und einem „Security Awareness Programme“ als neues Element ein Supply Chain Manager favorisiert, der die Sicherheit der Kette garantiert.

---

Die erwarteten Kosten liegen pro Unternehmen im Durchschnitt zwischen 5000 € p.a. (Kleinunternehmen) bis zu 300.000 € p.a. (Unternehmen mit mehr als 250 Mitarbeitern).

- Ein eigenes Forschungs- und Entwicklungsprogramm zu Sicherheitsthemen, das von der Europäischen Kommission im Rahmen des 7. F&E-Rahmenprogramms aufgelegt werden soll.

## 6 Resümee

Einigkeit besteht darüber, dass sowohl durch die bereits eingeführten Maßnahmen als auch durch zusätzliche Vorschriften niemals eine garantierte vollständige Sicherheit im Containerverkehr erzielbar ist. Eher scheint ein Vergleich mit dem Virusschutz für Computer angebracht: für jedes neue Virus wird sofort ein Virenschanner entwickelt, der „IT-Terroristen“ dazu anspricht, neue Viren zu entwickeln usw. Übertragen auf den Containerverkehr würde das heißen: Terroristen werden stets in der Lage sein, Mittel und Wege zu finden – nur die Schwelle entdeckt zu werden, wird ständig erhöht.

Maßnahmen und Initiativen existieren zurzeit noch partiell; die Ausweitung auf die gesamte Transportkette (über alle Verkehrsträger, über alle Staaten, um Wettbewerbsverzerrungen zu vermeiden) steht unmittelbar bevor. Hierbei ist sowohl die Gesetzgebung (Intermodal security directive) wie auch die technologische Ebene (elektronisches Siegel) zu sehen. Die Balance zwischen den Maßnahmen und den zugehörigen Kosten zu finden sowie klare Zuständigkeiten zu definieren, werden die großen Herausforderungen für Politik und Wirtschaft darstellen. Erstrebenswert sind Lösungen, die in einem Ansatz sowohl die Sicherheit erhöhen als auch logistische Prozesse optimieren; die könnte z.B. durch den Einsatz von RFID-Transpondern am Container und im elektronischen Siegel erreicht werden.

Eines haben die Terroristen des 11. September 2001 bereits geschafft: der volkswirtschaftliche Schaden, beziffert durch die Aufwände für neue Sicherheitsmaßnahmen (z.B. durch die Einführung des ISPS-Codes in Häfen und Reedereien), Konferenzen und Tagungen, Pilottests mit neuen Technologien, etc., die ohne diese Anschläge sicherlich nicht in dieser Geschwindigkeit und Intensität durchgeführt worden wären, ist beträchtlich.

## 7 Schrifttum

[CHCP04] Cargo Handling Cooperative Program (CHCP): Container Seal Technology and Processes, 2004

[DNV05] DNV consulting: Study on the impacts of possible European legislation to improve transport security, Final Report: Impact Assessment, Rev. 2, Antwerpen/Brüssel 2005

[EUR04] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Gefahrenabwehr in Häfen, KOM(2004) 76 endgültig, 2004/0031 (COD) vom 10.2.2004

[EVE03] Evens, Susan/de Bruijn, Ed: Technology in practice, Vortrag auf der Container Shipping Security Conference Antwerpen 2003

[HOL03] Hollmann, M.: Hinter elektronischen Schlössern, DVZ Nr. 146 vom 6.12.2003, S. 24

[IMO93] International Maritime Organisation: International Convention for Safe Containers (CSC), 1993 Edition

[IMO03] International Maritime Organisation: The International Ship and Port Security Code, 2003 Edition

[ISL05] Institut für Seeverkehrswirtschaft und Logistik, Shipping Statistics Yearbook 2004, Bremen 2005

[WOL02] Wolfe, M.: Freight Transportation Security and Productivity, Executive Summary, Intermodal Freight Security and Technology Workshop Long Beach, California, April 2002

[WOL03] Wolfe, M.: Automating Cargo Security: do electronic Seals Make Sense?, eyefortransport, February 12, 2003

Institut für Seeverkehrswirtschaft und Logistik Institute of Shipping Economics and Logistics		
<hr/>		
<b>Dr. Frank Arendt</b> Direktor		
Informationslogistik	Universitätsallee GW1 Block A 28359 Bremen Germany Fax +49/4 21/2 20 96-55	
Tel. +49/4 21/2 20 96-17 arendt@isl.org	www.isl.org	