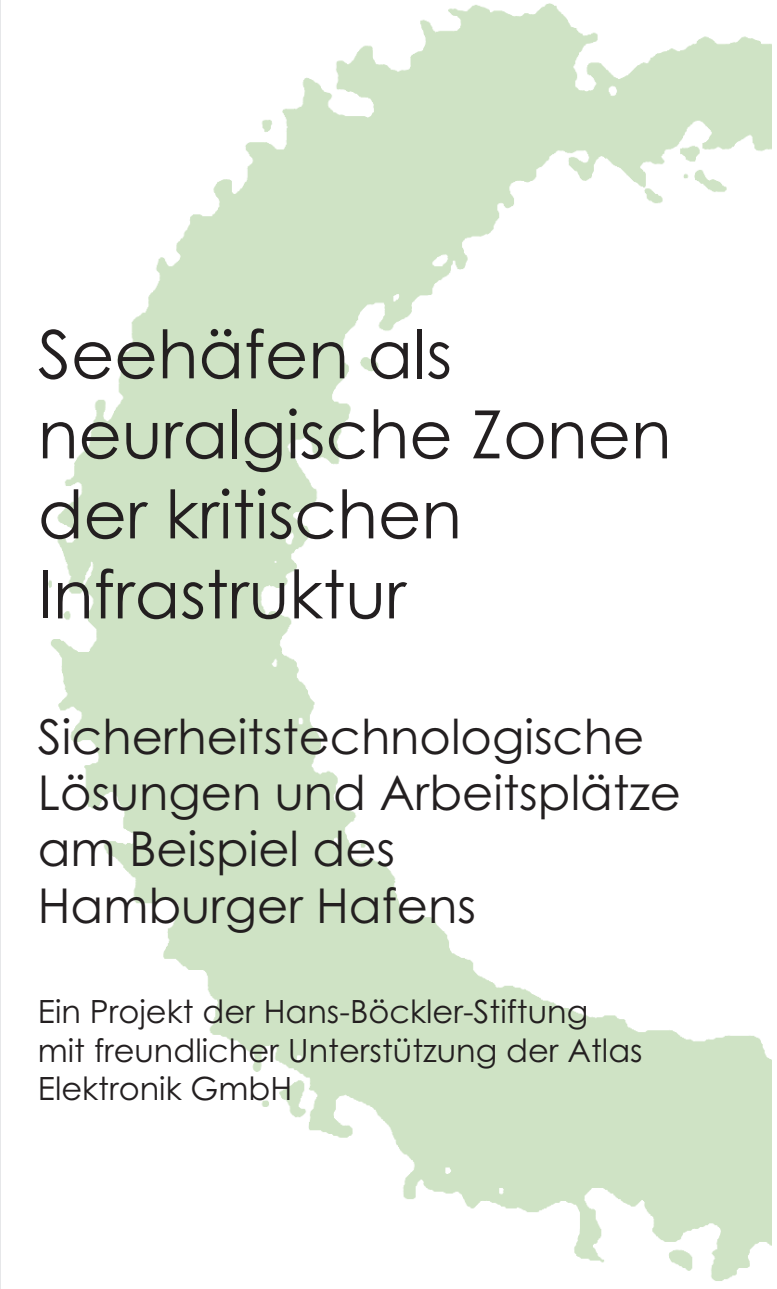
Bonn International Center for Conversion
B·I·C·C



Seehäfen als neuralgische Zonen der kritischen Infrastruktur

Sicherheitstechnologische Lösungen und Arbeitsplätze am Beispiel des Hamburger Hafens

Ein Projekt der Hans-Böckler-Stiftung
mit freundlicher Unterstützung der Atlas Elektronik GmbH

ENDBERICHT

BONN INTERNATIONAL CENTER FOR CONVERSION

B·I·C·C

Seehäfen als neuralgische Zonen der kritischen Infrastruktur.

Sicherheitstechnologische Lösungen und Arbeitsplätze am Beispiel des Hamburger Hafens.

Endbericht

abgeschlossen am 30.5.2008

HBS-Projektnummer 2008-99-1

Dr. Hartmut Küchle (Projektbearbeiter)
E-mail: kuechle@bicc.de
Bonn, 30. Mai 2008
Tel: 0228-91196-60

INTERNATIONALES KONVERSIONSZENTRUM BONN -
BONN INTERNATIONAL CENTER FOR CONVERSION (BICC) GMBH

Geschäftsführer: Peter J. Croll
Aufsichtsratsvorsitzender: Staatssekretär Dr. Michael Stückradt
Handelsregister: Bonn HRB 6717

An der Elisabethkirche 25
53113 Bonn
Tel.: +49-228-911 96-0
Fax: +49-228-24 12 15
E-Mail: bicc@bicc.de
Internet: www.bicc.de

Inhalt

1. Was ist Sicherheit? 3
2. Seehäfen als neuralgische Sicherheitszonen 7
3. Bedrohungen 9
4. Sicherheitstechnologische Lösungen 13
5. Unternehmen 18
5.1. Schenker 18
5.2. Atlas Elektronik 19
6. Arbeitsplatzpotenzial 23
7. Schlussfolgerungen 26

Gesprächspartner 29
Literatur 30

1. Was ist Sicherheit?

In der Theorie der Internationalen Beziehungen wurde Sicherheit entweder als eine relative Bedingung der Gegenwart oder als eine absolute Bedingung der Zukunft diskutiert. Daraus ergeben sich zumindest zwei Implikationen. Zum einen wird Sicherheit verstanden als etwas, das objektiv gekannt und deshalb mittels Vernunft und wissenschaftlicher Untersuchung gemessen, beobachtet und verbessert werden kann. Zum anderen erhält Sicherheit eine normative Qualität: sie erscheint als eine gute Sache, die wir aktiv anstreben sollten (von Boemcken, 2008).

Aus dieser Sicht ergibt sich die allgemeine Definition von Sicherheit aus der Abwesenheit oder zumindest der Unwahrscheinlichkeit der Bedrohung eines bestimmten Objekts (Baldwin 1997; Krause und Nye, 1975). Um jedoch vom Wesen der Sicherheit zu einem Konzept von Sicherheit zu kommen, ist die wichtigste Frage: Sicherheit für wen? In den meisten Fällen wird sich die Antwort auf Individuen oder Staaten beziehen. Es sind jedoch auch andere Objekte denkbar, wie z.B. die Biosphäre oder die Infrastruktur (von Boemcken, 2008).

Um den Gegenstand der Sicherheit näher zu spezifizieren kann es notwendig sein, nicht einfach nur auf die aktuell Sicherheit suchende Entität zu verweisen, sondern auch die gefährdeten Werte zu identifizieren, die diese bestimmte Entität repräsentiert. Beispielsweise kann ein Mensch mit verschiedenen Werten assoziiert werden, die alle schützenswert sein mögen. In diesem Fall muss ein Sicherheitskonzept klären, ob es sich auf körperliche Integrität, ökonomische Wohlfahrt, Autonomie oder psychologisches Wohlbefinden bezieht. Schließlich führen unterschiedliche Objekte und Werte zu ziemlich unterschiedlichen Konzeptualisierungen von Sicherheit, deren wichtigste natürlich „menschliches Leben“ und „staatliche Souveränität“ sind.

Des Weiteren könnte man über das Streben nach Sicherheit nachdenken. Hierzu hat Baldwin eine Reihe relevanter Fragen aufgeworfen. Zunächst sollten in Abhängigkeit vom konkreten Anliegen die Bedrohungen der Sicherheit identifiziert werden. Sodann sollte gefragt werden, welche Mittel und Strategien angewandt werden sollten, um diese Bedrohungen zu minimieren oder gar zu beseitigen. Sollen militärische Zwangsmaßnahmen angewandt werden oder doch eher zivile, entwicklungspolitische Maßnahmen, die auf die zugrunde liegenden Ursachen gerichtet sind? Dann muss

überlegt werden, wie viel Mittel für ein Mehr an Sicherheit verwandt werden sollten (Baldwin, 1997).

Schließlich wäre zu fragen, wer die Sicherheitsleistungen zu erbringen hat (Rothschild, 1995). Sind die staatlichen Institutionen immer am besten dafür geeignet oder könnte auch der private bzw. nicht-staatliche Sektor eine wichtige Rolle spielen?

Wenn man Sicherheit sowohl als objektive Existenzbedingung als auch als objektives Politikziel begreift, ergibt sich das folgende Schema (s. Abbildung 1).

Abbildung 1: Verschiedene Facetten von Sicherheit

Essence of Security	Objective condition described by the absence or low probability of threats to a certain object.
Concept of Security	Who is to be secured? Which values are to be secured?
Governance of Security	What are the threats to security? By which means and strategies is security to be achieved? How much resources should be devoted to security? Who is to do the securing?

Quelle: von Boemcken, 2008.

Eine etwas andere Perspektive erhalten wir, wenn wir fragen, was Sicherheit bewirkt. Dann werden Sicherheit und Unsicherheit nicht betrachtet als verbundene Existenz-bedingungen, die objektiv da sind und sich uns darbieten als unzweifelhafte Tatsachen des Lebens. Stattdessen werden sie dann verstanden als gesellschaftlich herausgebildet durch bestimmte Akteure und für jeweils besondere Zwecke. Nach dieser Sicht muss Sicherheit verstanden werden als intersubjektive gesellschaftliche Praxis, als etwas, das die Menschen selbst bewirken. Sicherheit ist damit eine besondere gesellschaftliche Kategorie, die aus der politischen Praxis entsteht (Waever, 2000).

Solch eine „konstruktivistische“ Betrachtung impliziert eine besondere Weise des Herangehens an Sicherheit. Sie beginnt nicht mit dem Identifizieren und Definieren der zugrunde liegenden, wesentlichen Bedeutung der Sicherheit, sondern beschränkt ihren analytischen Rahmen auf die diskursive und praktische Offenbarung des Begriffs im gesellschaftlichen und

politischen Leben. Sicherheit ist danach nicht mehr aber auch nicht weniger als das, was die Menschen sagen, das sie ist. Irgendwelche Probleme sind nicht von sich aus Sicherheitsprobleme. Sie werden es erst dann, wenn sie als solche benannt werden.

Daraus ergibt sich die Frage was passiert, wenn bestimmte Probleme als Sicherheitsprobleme behandelt werden. Die bekannteste Antwort darauf ist die von kritischen Sozialwissenschaftlern entwickelte „*Securitization*" („Versicherheitlichung") Theorie (Buzan, Waever und de Wilde, 1998). Damit meinen die Autoren die Abfolge verbindlicher Äußerungen, in denen ein konkretes Problem, sei es militärischer, politischer, wirtschaftlicher oder gesellschaftlicher Art, der Öffentlichkeit erfolgreich als existenzielle Bedrohung dargestellt wird, die dann ihrerseits Notstandsmaßnahmen fordert, die den normalen politischen Rahmen überschreiten und evtl. sogar die Verletzung etablierter Normen und Regeln legitimieren. *Securitization* macht also aus einem Problem ein *Governance*-Problem, das sich von bloßer Politisierung des Problems unterscheidet. Bei Letzterem wird der Prozess, durch den ein Problem in die öffentliche Debatte eingeführt wird, lediglich Teil eines *Bargaining* Prozesses im Kampf um finanzielle Ressourcen. Wenn dagegen ein Problem „securitized" bzw. „versicherheitlicht" wird, wird es als dermaßen dringend und existenziell dargestellt, dass es dem normalen Hickhack der Politik entzogen und auf eine Ebene jenseits der Mechanismen demokratischer Kontrolle gehoben zu werden droht (S. 29).

Die *Securitization* Theorie ist ein gutes Beispiel für den analytischen Wechsel von der Frage, was Sicherheit ist zu der Frage, was Sicherheit bewirkt. Dieser Wechsel bezeichnet eine fundamentale Veränderung der normativen Orientierung der Analyse. Denn da Bedrohungen nicht selbstevident, sondern immer Gegenstand der politischen Praxis sind, ist es eine bewusste und wohlüberlegte Entscheidung, ob gewisse Probleme als Sicherheitsprobleme adressiert und behandelt und damit „versicherheitlicht" werden. Die kritischen Autoren warnen davor, dies leichtfertig zu tun (Buzan et al., 1998).

Selbstverständlich kann über Sicherheit in der öffentlichen Debatte insbesondere der Innenpolitik gestritten und auf Maßnahmen gedrungen werden, ohne das betreffende Problem reflexartig in der eben dargelegten Weise einzuengen. Schließlich hat mit dem Terroranschlag vom 11. September 2001 eine Zäsur nicht nur im Bewusstsein der

Sicherheitspolitiker, sondern auch in der Realität stattgefunden, die zu negieren sträflich leichtsinnig wäre. Dennoch könnte die *Securitization* Theorie ein nützliches Analyseinstrument im Bereich der internationalen Beziehungen sein. Als Beispiel dafür wird von den kritischen Autoren auf den von den USA geführten „Krieg gegen den Terror" verwiesen. Hier sei das Problem dermaßen „versicherheitlicht" worden, dass schließlich drastische, über das notwendige Maß hinausgehende Gegenmaßnahmen einschließlich der Verletzung von Menschenrechten und internationalem Recht gerechtfertigt erschienen.

Diese theoretisch-philosophischen Betrachtungen zeigen zumindest wie notwendig es ist, bei einer Sicherheitsanalyse stets auch die engere Bedeutung von Sicherheit selbst und ihrer politischen Implikationen zu reflektieren. Dies dient sowohl der genaueren Spezifizierung des beabsichtigten Sicherheitskonzepts als auch der Sensibilisierung für die inter-subjektive Funktion von Sicherheit in der politischen Debatte (von Boemcken, 2008).

2. Seehäfen als neuralgische Sicherheitszonen

Zur kritischen Infrastruktur zählen Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen einträten. Dazu gehört vor allem auch die Verkehrsinfrastruktur (Bundesministerium des Innern, 2005). Eine der neuralgischen Sicherheitszonen der Verkehrsinfrastruktur stellen die Seehäfen dar. Das ergibt sich schon aus ihrer ökonomischen Bedeutung, wie das Beispiel des Hamburger Tiefseehafens zeigt.

Der Hamburger Hafen ist der größte Hafen Deutschlands, der drittgrößte in Europa und gehört als zweitgrößter Containerhafen Europas zu den neun größten Containerhäfen der Erde (Deutsche Verkehrs-Zeitung, 2001). 2007 wurden hier fast zehn Millionen Container umgeschlagen, zwölf Prozent mehr als im Jahr zuvor. 2008 wird mit einer weiteren Steigerung um 10 Prozent gerechnet. Trotz der fortgeschrittenen Containerisierung, die in Hamburg bereits einen Grad von 97 Prozent erreicht hat, verzeichnet der Universalhafen auch beim Stückgutumschlag ein deutliches Wachstum, er stieg um 9,1 Prozent. Fachleute rechnen mit einer Verdreifachung bis 2025 (Ritter, 2008).

12.000 Schiffe mit 121 Millionen NRT laufen jährlich den Hafen an. Er bietet Liegeplätze für 320 Seeschiffe, davon 38 für große Container- und Massengutfrachter. Weitere neun Liegeplätze für große Containerschiffe sind in Planung.

Im Hafengebiet sind 200 Betriebe angesiedelt, die rund 50.000 Mitarbeiter beschäftigen. Außer den Betrieben des Güterumschlags beherbergt der Hafen auch Werften und Raffinerien. Neben Mineralölfirmen und anderen Verarbeitungsunternehmen flüssiger Rohstoffe sind in Hamburg eine Reihe hoch spezialisierter Tanklagerbetriebe auf den Umschlag und die sichere Lagerung flüssiger Substanzen wie z.B. Fruchtsaftkonzentrate, Palmöl, Alkohol, Latex oder Säuren ausgerichtet.

An allen Umschlagsterminals zusammen wurde im Jahre 2007 die Rekordzahl von 140,4 Millionen Tonnen im Seegüterumschlag abgefertigt, das sind 4,1 Prozent mehr als im Vorjahr. Für 2008 wird mit einer Steigerung auf 146 Millionen Tonnen gerechnet. Dabei nehmen die Wachstumsraten mit großer Dynamik zu. Im Zeitraum 1991 und 1996 stieg der Hafenumschlag um 9 Prozent, von 1996 bis 2001 dagegen um

knapp 30 Prozent. In den letzten fünf Jahren verdoppelte sich der Güterumschlag im Hamburger Hafen. Prognosen gehen von einer weiteren Verdoppelung des Umschlagsvolumens bis zum Jahre 2015 auf ca. 222 Millionen Tonnen aus (Berenberg Bank - HWWI 2006; ;Planco Consulting GmbH 2007), und die Zahl der Standardcontainer (TEU) wird von heute 8,9 auf 18 Millionen im Jahre 2015 ansteigen[1]. Aufgrund dieser Entwicklung wird mit 14.000 neuen Arbeitsplätzen und 250 Millionen Euro an zusätzlichen Steuern pro Jahr gerechnet[2].

Hamburg bietet seinen Reedereikunden vier Container Terminals, sowie acht *Multi-Purpose* Terminals für den Boxumschlag. Es gibt mehr als 320 Liegeplätze und 41 km Kaimauern für Seeschiffe, rund 200 zum Teil computer-gesteuerte Containerbrücken sowie Löschanlagen für alle Arten von flüssiger Ladung.

Zwei Drittel der im Hamburger Hafen ankommenden Waren haben ihren Bestimmungsort außerhalb der Metropolregion Hamburgs[3]. Die logistische Leistung des Hamburger Hafens als einem der wichtigsten Umschlagplätze im weltweiten Verkehr besteht darin, dafür zu sorgen, dass an jedem Punkt der Transportkette die notwendigen Güter in der richtigen Menge, am richtigen Ort und zur richtigen Zeit zur Verfügung stehen.

Der Hamburger Hafen ist nicht nur ein Gewinner der deutschen Einheit, da er im Kalten Krieg von seinem Hinterland abgeschnitten war. Er ist auch ein Gewinner der Globalisierung. Der enorme Aufschwung Chinas, Indiens und Lateinamerikas und die Osterweiterung der Europäischen Union haben den internationalen Warenaustausch beflügelt, so dass sich der Hamburger Hafen zu einer der wichtigsten Drehscheiben des internationalen Güterverkehrs entwickeln konnte. Auf diesen Entwicklungen beruht die Schaffung von 2000 neuen Arbeitsplätzen sowie Steuereinnahmen von 900 Millionen Euro[4]. Mehr als 160.000 Arbeitsplätze hängen heute schon direkt und indirekt am Hamburger Hafen (Ritter, 2008).

1 Institut für Seeverkehrswirtschaft und Logistik in Bremen.
2 www.n-tv.de, 18.12.2007.
3 www.hafen-hamburg.de
4 Schiff & Hafen 2/2008, S. 26.

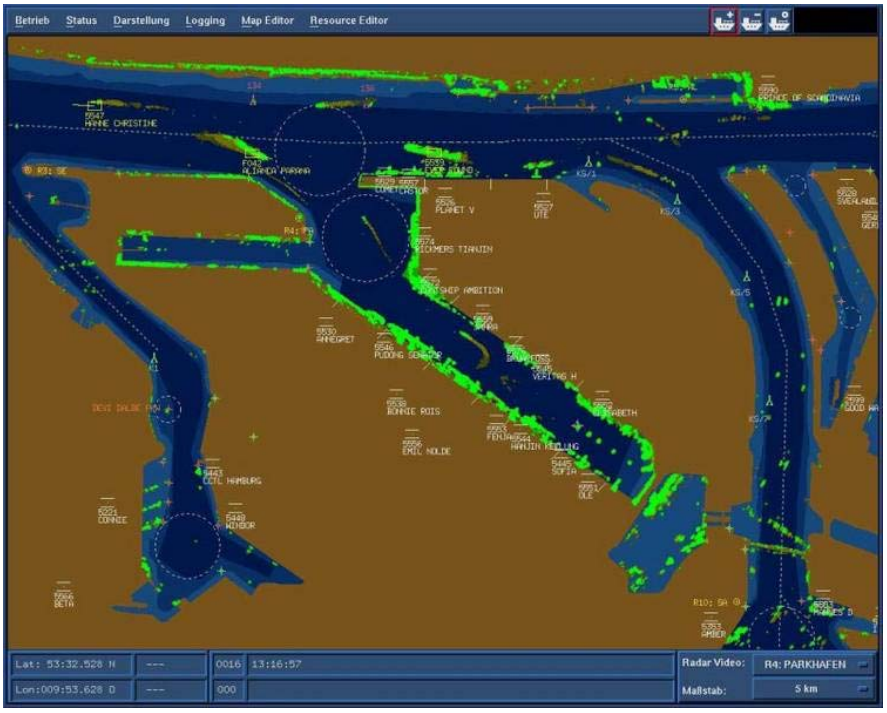
3. Bedrohungen

Wenn von Hafensicherheit gesprochen wird, ist vielfach die Sicherheit der gesamten maritimen Versorgungskette vom Ursprung der Güter bis zu ihrem Bestimmungsort gemeint (Haveman und Shatz, 2006). Dabei sind sehr viele verschiedene Akteure und Verladepunkte involviert, die ein Risiko darstellen können (US General Accounting Office, 2008). Wir wollen uns hier jedoch auf die Hafensicherheit im engeren Sinne beschränken. Dabei sind besonders zwei von Terroristen ausgehende Gefahren zu beachten: die direkte Bedrohung der Häfen selbst und die indirekte Bedrohung über den Transport gefährlicher Stoffe durch die Häfen für irgendwo geplante terroristische Anschläge (de Rugy, 2005). Seehäfen, Hafenanlagen, Schiffe, die den Hafen umgebende Infrastruktur und die durch den Hafen transportierten Güter haben jeweils unterschiedliche Verwundbarkeiten. Im Folgenden soll die Bedrohung der Schiffe im Mittelpunkt stehen, wobei zwei verschiedene Bedrohungslagen unterschieden werden:

- Bei langsamer Fahrt in den Hafen kann sich der Angreifer am Ufer, zu dem er freien Zugang hat, verbergen und auf das einlaufende Schiff warten.
- Beim Ruhen des Schiffes im Hafen muss sich der Angreifer dagegen auf den Hafen und das Schiff zu bewegen und dazu erstmal die Zugangskontrollen zum Hafengelände überwinden. Außerdem gibt es im Hafen eine gewisse Öffentlichkeit, die die „Arbeit“ der Terroristen erschwert, und die im Hafen vorhandenen Einrichtungen erleichtern die Rettung.

Der Hamburger Hafen liegt etwa 110 km von der Mündung der Elbe entfernt, gilt aber dennoch als Seehafen. Diese lange Elbmündung stellt ein zusätzliches Sicherheitsrisiko dar, da die Schiffe hier potenziellen Angreifern besonders ausgesetzt sind (s. Abbildung 2). Fachleute befürchten, dass die Hafeneinfahrt von Terroristen wochenlang blockiert werden könnte, indem einlaufende oder ankernde Schiffe mit ihrer wertvollen Fracht durch Sprengladungen zur Explosion gebracht werden. Ein brennender Tanker könnte so über den gesamten Hafen hinaus auch die Wirtschaft des ganzen Landes in Mitleidenschaft ziehen.

Abbildung 2: Der Hamburger Hafen



Quelle: www.atlas-elektronik.de

Das Absuchen der langen Elbmündung auf vermutete Minen dauert nach Auskunft von Experten etwa ein Vierteljahr[5]. Für eine Abschätzung der durch eine Hafenblockade entstehenden Schäden bzw. Kosten sind Studien zu den großen amerikanischen Häfen hilfreich, die schon öfters von Hurrikanen oder Streiks getroffen wurden. Sie zeigen, dass eine länger andauernde Schließung des Hafens die Wirtschaft der Stadt und der ganzen Region empfindlich treffen kann. Die Kosten hängen ab von der Dauer der Unterbrechung und von der Art wie flexibel die Reeder, Unternehmen und Konsumenten darauf reagieren. Schätzungen für die Kosten einer zehntägigen Blockade eines großen amerikanischen Hafens der Westküste variieren zwischen 500 Millionen US-Dollar und 19 Milliarden US-Dollar bzw. 58 Milliarden US-Dollar für die gesamte Volkswirtschaft (Martonosi, Ortiz und Willis, 2006). Die erhebliche Spanne zwischen den Schadenssummen beruht auf völlig unterschiedlichen Annahmen, wobei vor allem zwei Szenarien unterschieden werden: eine einwöchige und eine dreijährige Unterbrechung des Containerverkehrs (Congressional Budget Office, 2006). Eine Blockade, die länger als ein paar Tage dauert, hat einerseits höhere tägliche Kosten. Andererseits

[5] Der Suezkanal war nach seiner Verminung sogar 20 Jahre lang gesperrt (Expertengespräche).

können sich die wirtschaftlich Handelnden allmählich auf die Störung einstellen und nach Alternativen suchen. Außerdem muss zwischen den betriebswirtschaftlichen Kosten vor Ort und den makroökonomischen Kosten für das ganze Land unterschieden werden. Vom Standpunkt der Volkswirtschaft gilt, dass die Kosten der direkt Betroffenen durch mögliche Gewinne an anderer Stelle teilweise kompensiert werden (Congressional Budget Office, 2006).

Im Prinzip können zwar die durch eine Hafenblockade ausfallenden Einkommen durch einen Multiplikatoreffekt verstärkt werden, indem die direkt Betroffenen ihre Ausgaben einschränken und dadurch die Einkommen anderer reduzieren. Bei diesem „*worst case*" müssten neben den direkten Kosten dann auch die Transaktionskosten und andere indirekte Kosten berücksichtigt werden. Im Hafen wären dies insbesondere erhöhte Umschlags- und Liegezeiten, Sicherheitsmaßnahmen und Lieferunsicherheiten. Die indirekten Kosten resultieren vor allem aus den Störungen der normalen Versorgungskette und auch von Verhaltensänderungen der wirtschaftlichen Akteure.

Diese indirekten Kosten werden jedoch nach Meinung einiger Experten in der Regel überschätzt, weil man unterscheiden müsse zwischen Ereignissen, die wirtschaftliche Aktivitäten nur verzögern und solchen, die sie weitgehend unterbinden (Leamer und Thornberg, 2006). Hafenblockaden aufgrund von Streiks, Naturkatastrophen und Anschlägen hätten für die Wirtschaft des Landes keine statistischen Spuren hinterlassen etwa in Bezug auf Industrieproduktion, Konsumausgaben und Beschäftigung und zwar aus zwei Gründen. Einmal weil eine dynamische Marktwirtschaft an konjunkturelle, saisonale und andere Fluktuationen gewöhnt sei. Durch Störungen ausgefallene Produktion oder Käufe könnten nachgeholt werden. Zum anderen seien die Unternehmen flexibel und könnten alternative Bezugsquellen und Transportwege finden. Dazu komme ein weiterer Unterschied. Wirtschaftskrisen auslösende Ereignisse dauern mehrere Quartale und vermindern das Inlandsprodukt. Streiks, Naturkatastrophen oder Anschläge seien dagegen kurzfristig, regional beschränkt und gingen einher mit kompensierenden Nachfrageimpulsen für andere Güter und Dienstleistungen, so dass andere Unternehmen von der Blockade eines Hafens profitieren. Die statistischen Daten von Hafenschließungen in den Vereinigten Staaten ließen den Schluss zu, dass Störungen, die weniger als zwei Monate dauern, kaum in der Lage seien, ernsthaften indirekten wirtschaftlichen Schaden anzurichten.

Daraus folgern die Autoren, dass sich die auf den Schutz der Häfen gerichteten Sicherheitsmaßnahmen im Sinne einer Kosten-Nutzen-Analyse in vertretbarem Rahmen halten müssen. Die Kosten für eine erhöhte Sicherheit müssten mit dem dadurch verminderten Risiko in Einklang gebracht werden. Da die enorme Zahl von Containern mit der gegenwärtigen Technologie nicht zu 100 Prozent gescannt werden könne (Martonosi et al., 2006), sei es wichtiger, die Einschleusung von Massenvernichtungswaffen über den Hafen zu verhindern, als den Hafen selbst übermäßig zu schützen (Leamer und Thornberg, 2006).

Trotz dieser Relativierungen und trotz einer von manchen Experten als gering eingeschätzten Wahrscheinlichkeit, dass überhaupt ein Containerschiff für einen Terroranschlag benutzt wird (Haveman und Shatz, 2006), ist die Verwundbarkeit des Hafens und des maritimen Transportsystems zweifellos gegeben und der Schaden im Falle eines Falles extrem hoch. Allein schon die Tatsache, dass der Hamburger Hafen von einem dicht besiedelten Gebiet umgeben ist, sollte Grund genug für erhöhte Wachsamkeit sein. Die Nachricht, dass ein Maritim- und Hafenexperte 2004 zum Chef von Al Qaida in Saudi Arabien ernannt wurde (Haveman und Shatz, 2006), lässt durchaus mit dem Schlimmsten rechnen. Schließlich gibt es auch Experten, die die Zerstörungsgewalt, die von einem mit Flüssiggas beladenen explodierenden Tanker ausgeht, mit einem Atomschlag vergleichen. Alle Lebewesen im Umkreis von fünf km würden dabei ersticken, da die Explosion den gesamten Sauerstoff aufzehrt. Ein einfaches, aufblasbares Boot mit Sprengstoff beladen, könnte Auslöser eines derart vernichtenden Anschlags sein (Husick und Gale, 2005).

Die Bedrohungen gegen die Hafenanlagen und die Schiffe im Hafen und auf Reede können beispielsweise ausgehen von:

- Tauchern und Schwimmern,
- gekaperten Schiffen,
- Kleinflugzeugen aus der Luft und
- von Land her.

Dabei können sich die Terroristen verschiedener Wirkmittel bedienen. Dazu gehört vor allem Sprengstoff, besonders in Form von:

- ferngesteuerten Haftminen am Schiffsrumpf unter der Wasserlinie, aber auch
- Unterwasserminen in der Hafeneinfahrt und Landminen im Hafengelände (Truver, 2008).

4. Sicherheitstechnologische Lösungen

Allen Experten ist klar, dass sich Anschläge nicht völlig verhindern lassen. Ebenso klar ist jedoch, dass man mit Sicherheitstechnologien sowohl die Hürden für Anschläge als auch das Risiko für die Angreifer erhöhen kann. Abschreckung sei hier die beste Verteidigung, deshalb müsse man so viel absichern wie möglich.

Die Aufgabe Überwachung und Schutz des Hafens bezieht sich auf verschiedene Unterbereiche, beispielsweise auf das Hafengelände, die Anlagen und den Unter- und Überwasserbereich der Schiffe. Sicherheitstechnologische Lösungen werden vor allem gesucht für:

- die Zugangskontrolle zum Hafengelände,
- die Detektion von Sprengstoffen,
- die Vernetzung der unterschiedlichen Sicherheits-behörden,
- die Fracht- und Containerkontrolle und
- den Schutz der sich im Hafen befindenden Schiffe.

Die ersten vier Bereiche erfordern Technologien und Lösungen wie sie in ähnlicher Weise auch bei Flughäfen und vergleichbaren Verkehrsknotenpunkten zum Einsatz kommen und bereits im Rahmen einer anderen Studie beschrieben wurden (Küchle, 2008). So müssen die unterschiedlichen Behörden (Hafenverwaltung, Polizeien Niedersachsens, Hamburgs oder Schleswig-Holsteins) mit ihren jeweils unterschiedlichen Zuständigkeiten vernetzt werden mit dem Ziel einer gemeinsamen Lagedarstellung aller involvierten Behörden. Dafür kommen Informations- und Kommunikations-technologien in Frage.

Für den Frachtverkehr, der zu über 90 Prozent aus Containern besteht – von denen aber in der Regel nur 2 Prozent durchleuchtet werden – sind elektronische Verschlüsselungs- und Trackingverfahren zu entwickeln. Die Hongkonger Hafenbehörden testen Technologien, die jeden Container scannen durch gleichzeitigen Einsatz von Gammastrahlen und Strahlungsdetektion, ohne seinen Inhalt zu entfernen. Man erhofft sich davon einen 100 prozentigen Kontrolleffekt. Dieses noch in der Demonstrationsphase befindliche System muss jedoch zusammen mit traditionellen Kontrollsystemen verwendet werden, um vollständige Sicherheit zu gewährleisten. Auch das *US-Department of Homeland Security* forscht und arbeitet an fortgeschrittenen Technologien, um die Containerfracht zu überwachen und physisch zu sichern. In einem Pilotprogramm des New Yorker Hafens enthielt jeder

verfolgte Container eine *Black Box*, die aus fünf Sensoren besteht, die die Position eines jeden Containers durch zellulare Kommunikation und GPS (*global positioning satellites*) verfolgt. Damit konnte auch überwacht werden, ob der Container geöffnet wurde, Licht eingedrungen war, sich die Temperatur verändert hat[6] oder Strahlung herrschte. Wenn solche oder ähnliche Technologien entlang der gesamten Versorgungskette installiert würden, könnte die weltweite Transportsicherheit deutlich erhöht und Investitionen in innovative Technologien gefördert werden (The Port Authority of NY and NJ, 2006).

Wegen des Risikos des verdeckten Einschleusens von Gefahr- und Explosionsstoffen ist eine genaue Festschreibung der Frachtinformationen bei der Verladung von entscheidender Bedeutung (Bernnat, 2004; Emery, Werchan und Mowles, 2006; Klein, 2007). Dabei wird heute der Entwicklung einer neuen Generation von Sensoren große Aufmerksamkeit gewidmet, um in Containern verborgene chemische, biologische, radiologische oder nukleare Massenvernichtungswaffen zu entdecken. Diese gibt es in der gewünschten Form bisher nicht. Die natürliche Strahlung der Güter müsste unterschieden werden können von Stoffen, die missbräuchlich unter die Ladung gebracht wurden und Schaden verursachen können[7].

Es sind vor allem sechs Schlüsseltechnologien, die zu einer erhöhten Sicherheit im Hafen und im Containerverkehr beitragen: Sensortechnologien, Identifizierungs- und Autentifizierungstechnologien, Frachtkontrolle mit Durchleuchtungsgeräten *(Screening)*, Überwachungstechnologien (*Surveillance*), Ortungstechnologien (*antitamper*, *tracking and inspection*) und Technologien für integrierte Lösungen und Datenanalyse (Stowsky, 2006). Auch bei den zum Schutz des Hafens notwendigen Detektionssystemen, der Verifikationstechnik und Videoüberwachung kann auf bereits erfolgte Untersuchungen verwiesen werden (Küchle, 2008).

Schwerpunkt der vorliegenden Studie sollen deshalb Technologien sein, die dem Schutz der Schiffe im Hafen dienen. Dabei kommt es neben der Überwachung des Schiffverkehrs in Verbindung mit dem Hafenmanagement vor allem darauf an, sowohl die Wasseroberfläche als auch den

---

6 Hier zeigt sich, dass diese Technologie auch erhebliche wirtschaftliche Bedeutung z.B. für den Transport von Südfrüchten und anderer leicht verderblicher Ware hat.

7 Mit solchen Sensoren könnte auch das Entweichen gefährlicher Stoffe von Industriefirmen erkannt werden.

Unterwasserbereich des Schiffes zu überwachen. Geforscht wird nach hochauflösenden Radar- und Sonarbildern, die auch kleinere, schnell bewegliche Ziele wie z.B. Schnellboote, Taucher etc. aus sicherer Distanz entdecken, die notwendigen Zielparameter liefern und entsprechende Gegenmaßnahmen unterstützen. Zielgröße, Geschwindigkeit, Spur und mögliche Ausweichmöglichkeiten des Eindringlings werden in Echtzeit benötigt, um den Sicherheitskräften eine Reihe verschiedener Handlungsoptionen zu bieten[8].

Z.z wird besonders intensiv an folgenden Schutztechnologien gearbeitet:

- Aktiv und passiv arbeitende Unterwassersensoren zur Detektion von Tauchern;
- Abbildende Sensoren, Radar- und Positionssensoren, physikalisch-chemische Sensoren und akustische Sensoren;
- Sensoren und Unterwasser-Miniroboter zur Aufklärung des Unterwasserschiffes sowie des Meeresbodens unter dem Schiff und zur Aufklärung des Unterwasser-bereiches von Pieranlagen;
- Autonome Unterwasser-Fahrzeuge (AUV's) zur Detektion und Klassifikation von Seeminen in Hafen-zufahrten und auf Reeden;
- Akustische Detektionssysteme;
- *Automatic Identification Systems* (AIS).

Die bisher vorhandenen Systeme zum Schutz von Einrichtungen stellen meist isolierte Lösungen dar. Deshalb sind die aktuellen Bemühungen auf ein dreidimensionales Schutzsystem gerichtet, das das Erkennen von Bedrohungen im Überwasser- und Unterwasserbereich, im lokalen Luftraum und beim Zugang von Land ermöglicht (Kleinert und Nitsch, 2008). Die Aufstellung einzelner Sensoren ist dafür unzureichend. Da im Unterwasserbereich nur Sonar eingesetzt werden kann, Überwasser mit Optik und Radar und in der Luft nur mit Radar gearbeitet werden kann, besteht die Aufgabe darin, diese drei Dimensionen zu **einem** Bild zu vernetzen. Das Know-how zu dieser sogenannten Sensorfusion kommt vor allem aus dem militärischen Bereich. Die vernetzten Sensordaten müssen sodann in einer Einsatzzentrale zusammengeführt, dreidimensional dargestellt und ausgewertet werden. Es gilt, Personaleinsatz und vor allem Falschalarme weiter zu reduzieren.

---

8 www.atlas-elektronik.de

Darauf aufbauend bedarf es eines umfassenden Konzepts zum Hafenschutz, das auch geeignete Reaktionen bzw. Bekämpfungsmaßnahmen gegen entdeckte Terroristen einschließt. Grundlegend dafür ist der *System-of-Systems* Ansatz, der die Vernetzung der Sensoren und die verzugslose Darstellung der Daten einschließt. Die deutsche Industrie entwickelt hier im Auftrag der NATO das System LEXXWAR (*long-term experimental setup for asymmetric warfare*) zu einem mobilen, containerisierten System (Kleinert und Nitsch 2008). Deutschland hat im Rahmen der NATO die Führung übernommen für das Entwicklungsprogramm „*Technology for Intelligence, Surveillance, Reconnaissance and Target Acqusition of Terrorists* (ISRTA)".

Ein zentraler Entwicklungsschwerpunkt ist der Bereich maritimer Sicherheitssysteme und der Unterwasser-beobachtung. Hier sind Sonare die Schlüsselelemente für Hafenschutzsysteme[9]. Dabei lassen sich verschiedene Sonare unterscheiden:

- *Passive acoustic detection system*,
- *Remote underwater surveillance sonar sub-stations*,
- *Fairways and port entrance sonar systems*,
- *Pier-mounted active surveillance sonars,*
- *Ship-borne detection- and identification sonar,*
- *Underwater remotely controlled and autonomous vehicles carrying homing and identification sonar or high-resolution imaging sonar,*
- *Ship-borne bathymetric mapping and search sonar,*
- *Bottom-layed passive tripwire intrusion detectors,*
- *Combat divers' support sonar.*

Unbemannte Unterwasserfahrzeuge (UUV's), ferngesteuerte (ROV's) und autonome Unterwasserfahrzeuge (AUV's) können eine Vielzahl von Sensoren tragen, die verlässliche und umfassende Details für eine Bewertung der Bedrohungslage liefern. Damit können die Schiffsrümpfe intensiv und aus sicherer Entfernung auf Sprengladungen, aber auch auf Rauschgift und Schmuggelgut untersucht werden, die unter der Wasserlinie angebracht wurden. AUV's folgen autonom einem vorprogrammierten Such- und Handlungsmuster.

9 Sonare werden hauptsächlich für die Marine und nicht für zivile Zwecke produziert, obwohl sie für die Hafensicherheit wertvolle Dienste leisten könnten.

Fest installierte Hafenbeobachtungssonare entdecken sich bewegende Objekte wie z.B. Taucher und können benutzt werden, den Unterwasserrumpf ein- und auslaufender Schiffe zu überwachen. Ferngesteuerte oder autonom agierende Unterwasserfahrzeuge (ROV / AUV) dienen als bewegliche Sensorträger oder zur Beseitigung von gefährlichen Stoffen und Objekten. Eingebunden in ein Informationsnetzwerk soll den Nutzern ein stets aktuelles Lagebild zur Verfügung stehen. Auch die Anbindung weiterer Sensoren, TV-Kameras oder Nachtsichtsysteme wird angestrebt. Bei der Minenbekämpfung ist der Einsatz von unbemannten Unterwasserfahrzeugen bereits die Praxis. Ferngelenkte und autonom operierende Unterwasserfahrzeuge mit der Fähigkeit zur Detektion und Vernichtung von Minen können auf fast jeder Plattform mitgeführt werden[10].

[10] www.atlas-elektronik.de

5. Unternehmen

5.1. Schenker

Als Beispiel für die vielen Unternehmen, die sicherheitstechnologische Lösungen entwickeln, ohne eine Elektronikfirma oder ein wehrtechnisches Unternehmen zu sein, ist die Logistikfirma Schenker. Sie arbeitet an einer neuen Sicherheitstechnik, mit der erstmals Seefrachtcontainer lückenlos überwacht werden können. In „Schenker-smartboxes" werden Container neben RFID-Technik (*Radio Frequency Identification*) auch mit speziellen Sensoren (*GPS security devices*) ausgestattet. Die neuen GPS-Sensoren informieren in regelmäßigen Abständen über die Bedingungen und Sicherheitsparameter im Container wie Temperaturschwankungen, Erschütterungen oder Türaktivitäten, Aufenthaltsort und Route. Zum Beispiel kann die Temperatur für Pharmaprodukte und andere empfindliche Güter ständig überwacht werden, was sich langfristig als günstiger erweisen kann als der Transport in Kühlcontainern[11].

Darüber hinaus nimmt bei Schenker das *Tracking* in der Logistik einen immer höheren Stellenwert ein. Als Vorteile des *Trackings* werden genannt:

- Verfolgung der Sendung über das Internet;
- Einfacher und direkter Zugriff für alle Verkehrsträger – weltweit;
- Detailliertere Sendungsdaten;
- Rückverfolgbarkeit der vorangegangen Abläufe bzw. Ereignisse;
- Erreichbarkeit 24-Stunden an 7 Tagen;
- Erhöhte Transparenz für den Status der Sendung;
- Erhöhte Planungssicherheit.

Für den Produktbereich Seefracht bietet Schenker die erweiterte Tracking-Lösung *Customer Information Service* (CIS) an[12].

11 Griephan-globalsecurity 1/2008, S. 7.

12 www.schenker.de

5.2. Atlas Elektronik

Die Atlas Elektronik Gruppe arbeitet an Lösungen im und auf dem Wasser sowohl für zivile als auch militärische Anwendungen. Die Firma hat eine führende Position in allen Feldern der maritimen Hochtechnologie, von Vermessungsecholoten bis Schwergewichtstorpedos, vom Küstenschutz bis Minenjagdsonaren und von Führungssystemen inklusive der Funk- und Kommunikationsanlagen für U-Boote, Überwasserschiffe und Minenjagdboote bis hin zum Service vor Ort. Das Hauptwerk ist in Bremen. Ein weiteres größeres Werk sitzt in Wedel bei Hamburg. Das Unternehmen hat eine mehr als hundertjährige Geschichte. Es wurde 1911 als Atlas-Werke AG in Bremen gegründet und geht zurück auf eine 1843 errichtete Eisengießerei und Maschinenbauanstalt. Zu Beginn waren die Atlas-Werke auch ein Werftbetrieb, in dem nach dem Ersten Weltkrieg auch schiffstechnische Apparate hergestellt wurden. Ab 1964 gehörte das Unternehmen zum Krupp-Konzern. 1991 wurde die Krupp Atlas Elektronik in den Bremer Vulkan-Verbund eingegliedert. Nach dem Konkurs des Werftenverbundes gehörte die STN Atlas Elektronik zum Rheinmetall-Konzern. Ende 2005 wurde das Unternehmen dann von Thyssen-Krupp und dem europäischen Luftfahrt- und Militärtechnikkonzern EADS gekauft[13].

Der Elektronikspezialist für maritime Systeme verfügt über Produkte, die auf der Funktionskette vom Sensor bis zum Effektor basieren. Dadurch hat Atlas eine führende Rolle im neuen und stark wachsenden Markt der asymmetrischen Bedrohung, zusammengefasst unter dem Begriff "*Maritime Security*". Funk- und Kommunikationsanlagen von Atlas verbinden Marineschiffe und landgestützte Einrichtungen zu einem netzwerkbasierten Umfeld.

Die grundlegende Verfahrenstechnik und das Know-how in Sensoren, Signalverarbeitung, Führungs- und Kontrollsystemen und in Unterwasserfahrzeugen hat das Unternehmen in eine führende Position nicht nur bei Navalsystemen gebracht, sondern auch in benachbarten Märkten, wo diese Technologie bei anderen Anwendungen eingesetzt wird. Der Markt für Schiffsverkehrsüberwachung ist eines der Beispiele. Mit über 100 im Einsatz befindlichen Schiffsverkehrs-Überwachungssystemen und mehreren Küstenüberwachungssystemen hat die Firma nach eigener Einschätzung eine signifikante Position im Weltmarkt zur Überwachung von Wasserstraßen, Häfen und Küsten erworben.

---

13 www.atlas-elektronik.de

Besonders die ausgeprägten Unterwassertestanlagen mit einem Akustikbecken, instrumentierten Versuchssee und besonders ausgerüstete Versuchsschiffe ermöglichen es Atlas, Ingenieurs- und Fertigungslösungen abzuliefern. Bei Sensoren steht u.a. die gesamte Palette an Aktiv- und Passivsonaren vom klassischen Bugsonar bis zu modernen Schleppsonaren zur Verfügung. Atlas besitzt auch Fähigkeiten in der Minenjagd. Komplette Minenjagdsysteme, vom Sonar bis zu autonomen oder ferngelenkten Unterwasserfahrzeugen zur Minenvernichtung, wurden an die Deutsche Marine und an viele internationale Marinen mit Minenjagdfähigkeiten geliefert.

Beispielhaft seien hier einige herausragende, für die Hafensicherheit relevante Produkte aus dem Hause Atlas erwähnt:

Seefuchs I: Der Seefuchs ist geeignet für das Orten von Sprengstoffen, die am Meeresgrund oder in bedrohlicher Nähe zu Schiffen platziert sind, und für die Inspektion von Schiffsrümpfen und umliegenden Ankerplätzen. Die Nutzlast für die Bodenvermessung ist ein Randabtastsonar (*side scan looking sonar*). Für das Inspizieren von Schiffsrümpfen kann ein aufwärts lotendes Sonar und ein TV-Kamerasystem integriert werden, noch aufgewertet durch ein Laserabtastsystem zur dreidimensionalen Identifikation von am Schiffsrumpf angebrachten Objekten. Der Atlas Seefuchs I ist ein kleines und leichtgewichtiges unabhängiges Unterwasser-fahrzeug. Es ist bestückt mit einem Inertialnavigationssystem und einem 360° vorausschauenden Sonar für autonome Einsätze. Dieses kleine und leichte ROV gilt als vielversprechend bei der Bereitstellung von schneller Unterwasseraufklärung, Inspektion von Häfen, Pieranlagen, Zufahrtsgewässern und Ankerplätzen. Dieser Seefuchs ist die Grundversion einer immer weiter spezialisierten Reihe und wurde schon in einer Stückzahl von 1.500 produziert. Er kann den Unterwasserbereich nach Haftminen absuchen, ist allerdings bei schlechter Sicht eingeschränkt gegenüber Tauchern, die die verdächtigen Stellen notfalls auch abtasten können. Der Einsatz von Tauchern kostet allerdings ein Mehrfaches.

Der **Seefuchs IQ** ist ein vielseitiges Fahrzeug zur Identifikation, Inspektion und Überwachung. Es ist voll wiederverwendbar und ermöglicht so Einsätze bei sehr geringen Kosten. Durch seine Modularität kann das System für Trainings- und Idenfikationszwecke bei der Minenjagd, als auch beim Abfangen von Schwimmern oder Sondermissionen eingesetzt werden. Bei der riskanten Minenjagd kann das Fahrzeug mit

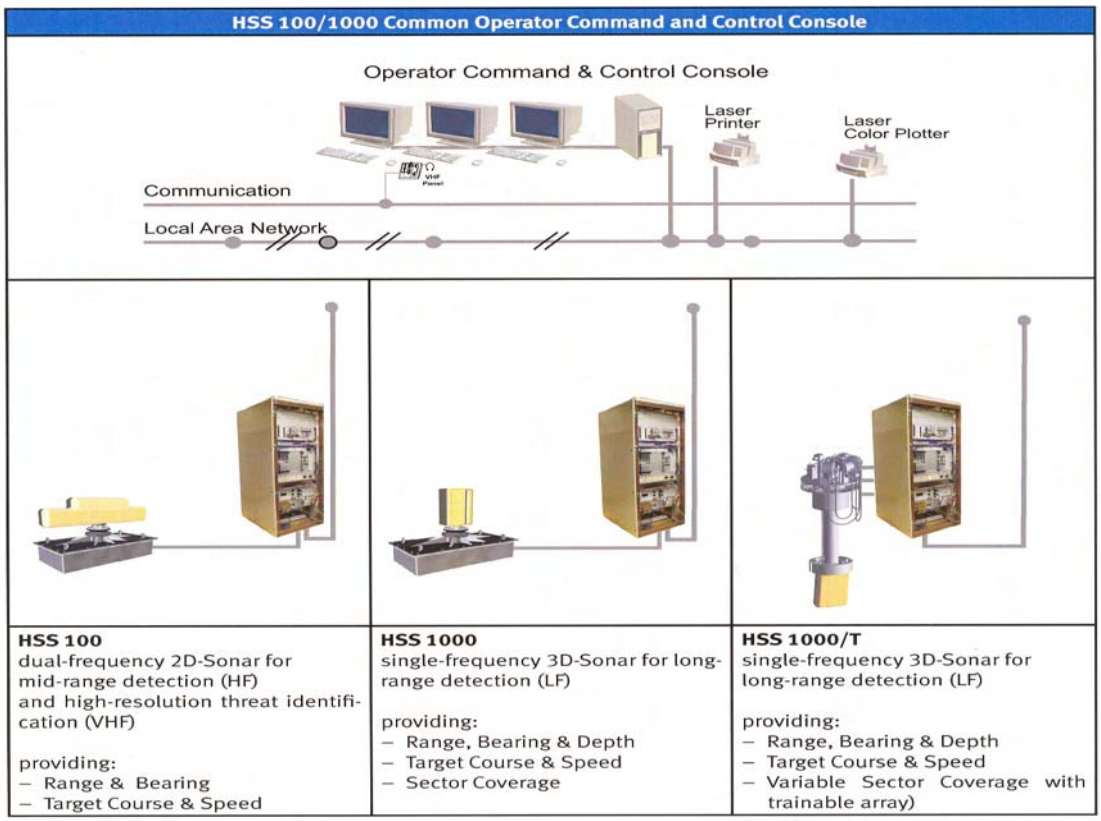
Billigsensoren und einer verankerten Kamera ausgerüstet werden. Für Inspektionsaufgaben, Vermessung und Taucherunterstützung, also bei kommerziellen Anwendungen, kann das Fahrzeug mit zusätzlichen Sensoren, inklusive Extra-Suchlicht, schwenkbare Kamera und Randabtastsonar ausgerüstet werden. Das System kann auf See oder landgestützt von verschiedenen Konsolen bedient werden, inklusive portabler Hartschalenkonsolenwagen.

Das bewährte AUV-System **Seeotter MkI** ist adaptiert an modernste Anforderungen in Navigationssoftware und Einsatzführung und ist das ideale System zum Schutze von Schiff und Hafen. Das Fahrzeug liefert präzise Positionsdaten, Stabilität und Beweglichkeit für eine genaue Datensammlung. Das Bordsystem stellt alle notwendigen Positionen, Statusmeldungen und Echtzeitinformationen bereit. Es garantiert somit eine effektive und ausgiebige Leistung während der gesamten Mission. Die hohe Positionsgenauigkeit und genaue Stabilisierung des Fahrzeuges während der Datenaufnahme erlaubt das Abbilden der Rohdaten in direkter Umsetzung ohne Nachverarbeitung oder das Einholen von notwendigen Korrelationspunkten bei Vermessungslücken speziell in einer komplexen Umgebung wie Häfen. Um den Anforderungen der Hafeninspektion gerecht zu werden, ist das AUV mit folgenden Basisnutzlasten bestückt: Randabtastsonar, Sedimentlot und Mehrfachstrahl-Echolot.

Das **Hafen-Überwachungssonar HSS-100/HSS-1000** bietet lückenlose Überwachung und Identifizierung von Angreifern und/oder der Unterwasserübergabe illegaler Güter oder Substanzen. Sichere Entdeckung, Identifizierung, Verfolgung und hocheffiziente Unterdrückung von Eindringlingen hält die Betriebsrisiken der maritimen Infrastruktur auf einem Minimum. Das Hafen-Überwachungssonar Atlas HSS-100/1000 ist eine vielseitige Familie von Sonaren zur Entdeckung und Verteidigung, die hochauflösendes 2D/3D-Sonar mit Zentimeterauflösung bietet. Davon stehen drei verschiedene Versionen zur Verfügung, von denen jede auf die individuellen Bedürfnisse verschiedener maritimer Sicherheitskräfte zugeschneidert ist. Alle Systeme ermöglichen eine sichere Entdeckung aktiver Unterwassereindringlinge ebenso wie passiver Bedrohungen wie Minen oder verdeckte Drogenlieferungen. Eine gemeinsame *Command and Control* Technologie ermöglicht es, komplexe Unterwasser-Überwachungssysteme mit einer Vielzahl von Sonar-Unteranordnungen zu konfigurieren, um auch größere Überwachungszonen abzudecken je nach individuellem,

lokalem oder regionalem Erfordernis. Die modulare Struktur unterstützt weiterhin die Integration verschiedener HSS 100/1000 Varianten in einem einzigen System. Eine eingebaute Testausrüstung überwacht kontinuierlich die Systemaktivitäten. Im Falle irgendeiner Fehlfunktion wird der Betreiber sofort benachrichtigt und erhält entsprechende Korrekturanweisungen. Auch eine langfristige Überwachung und Dokumentation steht zur Verfügung, um Wartung und Ersatzteillogistik zu unterstützen[14]. Abbildung 3 zeigt den Aufbau der *Command and Control Console* der HSS-100/1000.

Abbildung 3: Harbour Surveillance Sonar Atlas HSS-100/1000



Quelle: Atlas Elektronik, 2007, S. 8.

Daneben ist Atlas Elektronik führend bei *Vessel Traffic* Systemen, die jedoch in erster Linie für die Überwachung und Steuerung des Schiffsverkehrs und erst in zweiter Linie für die Hafensicherheit von Bedeutung sind.

[14] www.atlas-elektronik.de

6. Arbeitsplatzpotenzial

Der deutsche Markt für sicherheitstechnische Produkte und Dienstleistungen hatte im Jahre 2005 ein Umsatzvolumen von 10 Milliarden Euro – bei hohen Wachstumsraten. Ein Umsatzanstieg ist in allen Teilbereichen zu verzeichnen, und dieser Trend setzt sich fort (Staimer, 2007). Deutschland mit seinen starken Basistechnologien und einer vielfältigen Forschungslandschaft bringt gute Voraussetzungen mit, um im internationalen Wettbewerb auf diesem Zukunftsmarkt zu bestehen und neue Arbeitsplätze zu schaffen. Dafür ist es wichtig, dass die Sicherheitsfirmen nicht nur das Gerät allein verkaufen, sondern auch ein umfassendes Sicherheitskonzept und die entsprechende Organisation anbieten. Mit dieser Paketlösung, die von den großen Firmen bereits praktiziert wird, ist es aussichtsreicher, den gesamten europäischen Markt zu bedienen und die Beschäftigung in den deutschen Firmen zu sichern[15].

Die Atlas Elektronik Gruppe beschäftigt ca. 1.800 Mitarbeiter, von denen jedoch nur 80 bis 90 gewerbliche Mitarbeiter in der Produktion sind. Dabei handelt es sich um qualitativ hochwertige Arbeiten, die aus Sicherheits- und Qualitätsgründen nicht von außen zugekauft werden können. Dazu gehören beispielsweise die Messtechnik (Messung auf Dreikoordinatenmessgeräten KMG, Form-, Profil- und Lagemessung, Schichtdickenmessung, Glanzgrad, Oberflächengüte, Erstellung von CNC-Messprogrammen, Prüfung von Kleb-, Schweiß- und Nietverbindungen) und das Kalibrierlabor, die ihre Dienstleistungen auch anderen Firmen anbieten. Sowohl die gewerblichen Arbeitnehmer als auch die Ingenieure, die den überwiegenden Teil der Belegschaft bilden, sind Spezialisten im zivilen und militärischen Maritimbereich, deren Fähigkeiten den gesamten Produktlebenszyklus umfassen, von der Entwicklung über die Produktion bis hin zum Service vor Ort.

Atlas ist insbesondere bei Sonaren weltweit führend und hält zusammen mit dem französischen Konkurrenten Thales einen Weltmarktanteil von 70 Prozent[16]. Weitere Konkurrenten sind im Wesentlichen die Elektronikfirmen aus dem Rüstungsbereich, z.B. Raytheon (USA) oder Kongsberg (Norwegen). Im engen Bereich der Hafensicherheit heißt der europäische

15 Expertengespräche.
16 Expertengespräch.

Konkurrent Softwarelock, der zur EADS-Frankreich gehört und ca. 60 Beschäftigte hat[17].

Atlas Elektronik hat für die Hafensicherheit 25 Ingenieure in Bremen und weitere 35 Beschäftigte in Unterschleißheim, die ausschließlich Software entwickeln, während die Hardware eingekauft wird. Diese wenigen, aber hochqualifizierten Beschäftigten bewegen allerdings Projekte, die insgesamt viele Hundert Leute beschäftigen und ein Mehrfaches der Wertschöpfung erzeugen, die bei Atlas direkt entsteht. Beispielsweise ist Atlas mit etwa 20 Beschäftigten in Bremen verantwortlich für ein Projekt zur Überwachung des Schiffsverkehrs vor der portugiesischen Küste mit einem Volumen von 80 Millionen Euro. Davon entfallen 40-44 Millionen Euro auf Atlas, die andere Hälfte auf eine Reihe von Partnern, Subfirmen und Zulieferern[18]. Zu solchen umfassenden Gesamtpaketen mit einem riesigen Finanzvolumen gehören z.B. auch Baumaßnahmen, Erd- und Betonarbeiten und andere Arbeiten, die von einer Vielzahl in- und ausländischer Firmen ausgeführt werden. Deshalb ist ein Überblick über die gesamte Beschäftigung solcher Projekte oder auch einzelner Systemlösungen kaum möglich. Der allgemeine Trend ist jedoch klar. Alle befragten Unternehmen berichten übereinstimmend von einem zunehmenden Bedarf an Fachkräften auf allen Ebenen (Goericke, 2007). Insgesamt ist davon auszugehen, dass das wachsende Sicherheitsbedürfnis auch zu neuen und extrem hochwertigen Arbeitsplätzen in diesen Firmen führt.

Vor diesem Hintergrund erstaunt, dass Atlas von den 1.800 Beschäftigten in diesem Jahr trotz steigender Umsatzzahlen 300 Beschäftigte abbaut. Dies liegt zum einen daran, dass die bisher getrennten Abteilungen für unterschiedliche Sonarsysteme zu einer zentralen Sonareinheit zusammengelegt werden, um Synergieeffekte zu erzielen. In Gesprächen mit dem Betriebsrat wurde deutlich, dass der Abbau sozialverträglich durchgeführt wird, vor allem über Altersteilzeit[19]. Darüber hinaus ist zum 1. April 2008 eine neue, schlankere Organisation in Kraft getreten[20].

---

17 Expertengespräch.

18 Expertengespräche.

19 Daneben ist es dem Betriebsrat gelungen, dass wieder nach dem Flächentarifvertrag entlohnt wird; Expertengespräch.

20 Atlas Elektronik Newsletter, Ausgabe 1/2008.

Zum anderen verzeichnet Atlas trotz der seit dem 11.September 2001 erhöhten Priorität für Sicherheit keine markant steigende Nachfrage nach seinen technologischen Lösungen[21], obwohl alle Häfen der Welt vor ähnlichen Problemen stehen. Hier scheint noch Wachstumsspielraum zu bestehen, der durch industriepolitische Maßnahmen unterstützt werden sollte.

[21] Eine positive Ausnahme ist allerdings der Containerbereich; Expertengespräch.

7. Schlussfolgerungen

Die sicherheitsrelevanten Problem- bzw. Aufgabenbereiche im Bereich der Hafensicherheit sind an sich nicht neu. Es gab sie auch schon früher, sie haben aber seit den jüngsten Anschlägen an Bedeutung gewonnen. Die zur Verfügung stehenden Technologien sind ebenfalls nicht neu. Aber aufgrund des neuen Problembewusstseins hat sich in den letzten Jahren ein weltweiter Markt für diese Technologien entwickelt mit breitem Einsatzspektrum sowohl im zivilen wie im militärischen Bereich. Dadurch sinken in der Tendenz die Preise und befördern in vielen Fällen zusätzlich ihren Einsatz. Deshalb sollte die Entwicklung von *dual-use* Technologien gezielt vorangetrieben werden, um *economies of scale* und erhebliche Einsparpotenziale zu erreichen.

Deutschland zeichnet sich nicht nur durch starke Basistechnologien und eine vielfältige Forschungslandschaft aus und verfügt über zentrale Kompetenzen im Bereich der zivilen und militärischen Sicherheitstechnik, es verfügt gerade auf dem Gebiet der Hafen- und Schiffssicherheit über mindestens ein weltweit führendes Unternehmen und kompetente Zulieferer. Damit sind große Chancen auf diese Zukunftsmärkte gegeben. Diese müssen aber systematisch genutzt werden, um auch beschäftigungswirksam zu werden.

Daraus folgt die Notwendigkeit einer aktiven Industriepolitik. Diese sollte zunächst alle wichtigen Akteure in Forschung, Industrie und Politik vernetzen, um zu einer Clusterbildung zu kommen. Unternehmensübergreifende Cluster können helfen, klare Technologieschwerpunkte zu erarbeiten und die vorhandenen Kompetenzen und Fähigkeiten zu bündeln und auf gemeinsame Projekte auszurichten. Cluster bieten auch Informations- und Kostenvorteile, denn Synergien entstehen nur bei intensiver Kooperation. Durch eine wertschöpfungsorientierte, auch interdisziplinäre, Zusammenarbeit der Unternehmen sowie durch Forschungs- und Entwicklungskooperationen entstehen Innovationen, Produktivitätssteigerungen und schließlich wirtschaftliche Erfolge (Küchle, 2008). Wichtige Ansätze dazu sind in Form von Netzwerken bereits gegeben und sollten weiter ausgebaut werden.

Ebenso wichtig wie die gezielte Förderung der Forschung ist jedoch, die Forschungsergebnisse schneller als bisher in der Produktion zu realisieren und zu vermarkten. Deshalb sollten neu entwickelte Sicherheitslösungen zügig in deutschen Häfen implementiert werden, denn Referenzbeispiele sind oft eine grundlegende Voraussetzung für die weltweite Vermarktung. Private oder staatliche Hafenbetreiber sollten durch staatliche Industriepolitik angeregt werden, mehr für die Sicherheit zu investieren.

Unabhängig von staatlicher Förderung haben die Häfen allerdings auch ein Eigeninteresse. Ein mit neuesten Technologien gesicherter Hafen könnte nämlich teure Versicherungsprämien sparen und hätte dadurch und durch seinen hohen Sicherheitsstandard einen Wettbewerbsvorteil vor anderen Häfen. Das Gleiche gilt für entsprechend gesicherte Schiffe, die lange Liegezeiten wegen der sonst vorgeschriebenen Sicherheitschecks verkürzen könnten. Das wird in Vereinigten Staaten bereits erfolgreich praktiziert.

Schließlich könnte auch die Technologieförderung selbst verbessert werden. Der Umweg über Brüssel erscheint nicht gerade effizient und eher nachteilig für deutsche Unternehmen. Europäische Förderprojekte werden zwar zu einem erheblichen Teil von Deutschland alimentiert, jedoch aus nationalen Proporzgründen vielfach an ausländische Unternehmen vergeben, die nicht unbedingt kompetent sind bzw. diese technologischen Kompetenzen erst erwerben müssen. Das selbst gesetzte Ziel der EU-Kommission, Europas Forschung und Produktivität merklich zu steigern, wird auf diese auch bürokratischere Weise kaum erreicht. Vielmehr fällt Europa weiter gegenüber den Vereinigten Staaten zurück. Die deutschen Steuermittel, die über Brüssel umverteilt werden, könnten produktiver verwandt werden durch direkte nationale Förderung der deutschen Unternehmen, zumal diese europaweit und teilweise auch weltweit führend sind.

Eine strategische Industriepolitik könnte dafür sorgen, dass

- die deutschen Häfen sicherer gemacht würden und so einen internationalen Wettbewerbsvorteil hätten,
- der mit neuesten Sicherheitstechnologien aufgerüstete Hamburger Hafen weltweit als Musterbeispiel vermarktet wird,
- Technologien national und nicht über die Umverteilungsgießkanne Brüssel gefördert würden,
- Pilotprojekte gefördert werden, damit Firmen Erfahrungen sammeln können und
- die Bundesmarine mit den neuesten Technologien ausgerüstet würde, um so als Referenzbeispiel ihren Export weltweit zu fördern.

Gesprächspartner

- Ahlmann, Michael. Dipl.-Ing. Betriebsratsvorsitzender Atlas Elektronik Bremen.
- Duschka, Michael. Redakteur „Home and Security".
- Fischer, Hans-Martin. Geschäftsführer und stellvertretender Vorsitzender ZVEI –Zentralverband Elektrotechnik- und Elektronikindustrie e.V., Fachverband Sicherheitssysteme, Frankfurt am Main.
- Hornfeld, Willi. *Sales and Marketing. Autonomous Underwater Vehicles*, Atlas Elektronik Bremen.
- Kunze, Thomas. Systems Concepts, Maritime Security Systems, Traffic Control Systems & Harbour Security. Atlas Elektronik GmbH, Bremen.
- Lüders, Tom. *Program Manager Global Security, EADS Defence and Security Systems*, Unterschleißheim.
- Pieck, Stefan. H*ead of Security Services Defence and Communications Systems*, EADS Deutschland GmbH, Bonn/Berlin.
- Proske, Gebhard. *Executive Director Maritime Security Systems*. Atlas Elektronik GmbH, Unterschleißheim.
- Rehak, Dr. Wolfgang. Projektmanagement Optotransmitter-Umweltschutz-Technologie (OUT) e.V. Berlin.

Literatur

Atlas Elektronik. 2007. *Harbour Surveillance Sonar*. Bremen.

Baldwin, David A. 1997. "The Concept of Security." *Review of International Studies*, Bd. 23, Seiten 5-26.

Berenberg Bank - HWWI. 2006. *Strategie 2030 - Maritime Wirtschaft und Transportlogistik*. Hamburg, September.

Bernnat, Rainer. 2004. "Herausforderungen einer gesamtstaatlichen Sicherheitsarchitektur am Beispiel Homeland Security. " In: J. Vielhaber, Hrsg., *Homeland Security: Die Bedrohung durch den Terrorismus als Herausforderung für eine gesamtstaatliche Sicherheitsarchitektur*. Berlin: DGAP.

Bundesministerium des Innern. 2005. *Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informations-infrastrukturen*. Berlin, Referat Öffentlichkeitsarbeit.

Buzan, Barry, Ole Waever und Jaap de Wilde. 1998. *Security. A New Framework for Analysis*. Boulder, CO / London: Lynne Rienner.

Congressional Budget Office. 2006. *The Economic Costs of Disruptions in Container Shipments*. Washington, DC, The Congress of the United States, 29 March.

de Rugy, Veronique. 2005. *Is Port Security Spending Making Us Safer?* Washington, DC, 7. September.

Deutsche Verkehrs-Zeitung. 2001. "Transport- und Logistik-drehscheibe Hamburg " *Deutsche Verkehrs-Zeitung, [Sonderbeilage]* 28.04., S. 9-24.

Emery, Norman, Jason Werchan, und Donald G. Mowles. 2006. "Fighting Terrorism and Insurgery: Shaping the Information Environment." *Milirary Technology*, 11/2006, Seiten 104-110.

Goericke, Stephan. 2007. *Gründung eines GESA Workshops "Fachkräftequalifizierung". Zweite GESA-Konferenz*. Brüssel.

Haveman, Jon D. und Howard J. Shatz, Hrsg.. 2006. *Protecting the Nation's Seaports: Balacing Security and Cost*.

Husick, Lawrence A. und Stephen Gale. 2005. *Planning a Sea-borne Terrorist Attack*, Foreign Policy Research Institute, 21 March.

Klein, Adam. 2007. "The Costs of Terror: The Economic Consequences of Global Terrorism." *Analysen & Argumente (Konrad-Adenauer-Stiftung)*, 41, Mai.

Kleinert, Günter und Elke Nitsch. 2008. "Port and Harbour Protection." *Strategie und Technik*, April.

Krause, Lawrence und Joseph Nye. 1975. "Reflections on the Economics and Politics of International Economic Organisations. " In: Bergsten und Krause, Hrsg., *World Politics and International Economics*. Washington, DC: The Brookings Institute.

Küchle, Hartmut. 2008. *Innovationen zum Schutz deutscher Flughäfen vor Anschlägen. Sicherheitstechnologien und Arbeitsplätze am Beispiel des Düsseldorfer Flughafens*. Bonn, BICC, 5. Februar.

Leamer, Edward E. und Christopher Thornberg. 2006. "Ports, Trade, and Terrorism: Balancing the Catastrophic and the Chronic." In: J. D. Haveman und H. J. Shatz, Hrsg., *Protecting the Nation's Seaports: Balancing Security and Cost*. S. 31-62.

Martonosi, Susan E., David S. Ortiz, und Henry H. Willis. 2006. "Evaluating the viability of 100 per cent container inspection at America's ports." In: Rand Corporation, Hrsg., *The Economics of Terrorist Attacks*.

Planco Consulting GmbH. 2007. *Seeverkehrsprognose*. Berlin, Bundesministerium für Verkehr, Bau und Stadtentwicklung, April.

Ritter, Johannes. 2008. "Alles hängt am Hafen." *Frankfurter Allgemeine Zeitung*, 21. Februar., S. 11.

Rothschild, Emma. 1995. "What is Security?" *Daedalus*, Bd. 124, Summer, Seiten 53-98.

Staimer, Angelika. 2007. "Der Markt für elektronische Sicherheitssysteme in Deutschland 2006 - Daten, Tendenzen, Auswirkungen." Pressekonferenz des Fachverbandes Sicherheitssysteme.

Stowsky, Jay. 2006. "Harnessing a Trojan Horse: Aligning Security Investments with Commercial Trajectories in Cargo Container Shipping." In: J. D. Haveman und H. J. Shatz, Hrsg., *Protecting the Nation's Seaports: Balancing Security and Cost*. S. 31-62.

The Port Authority of NY and NJ. 2006. *Port Security Task Force Report*. New York, December.

Truver, Scott C. 2008. "Mines and Underwater IEDS in U.S. Ports and Waterways." *Naval War College Review*, Bd. 61, Nr. 1, Seiten 106-126.

US General Accounting Office. 2008. *Supply Chain Security. Report to Congressional Requesters*. GAO-07-626T. Washington DC, January.

von Boemcken, Marc. 2008. "Security. What does it mean? What does it do?" Bonn: BICC (im Erscheinen).

Waever, Ole. 2000. *Security agendas old and new, and how to survive them*. Buenos Aires, Universitad Torcuato di Tella.