

Sicherheit der Seewege – eine Betrachtung aus wirtschaftlicher Sicht

Philip Buse*

Abstract: The following text tries to show, by means of three examples, the challenge of maritime security for the economies of producing, distributing and consuming states, respectively. Considering the fact that over 90 per cent of all transported goods worldwide are carried by seagoing vessels, everybody understands the need to protect international transport routes against criminal acts and, more recently, terrorist attacks. One aspect of this is the protection of port facilities and stored goods, i.e. containers, as well as, the protection of the ships themselves. This should be met by the provisions of the ISPS Code. The second aspect is the surveillance and protection of goods using any other means of transport. The aim is the documentation of every part of the supply chain. The third and last aspect concerns the »traditional and common« piracy on seagoing vessels for either criminal or terrorist purposes and the countermeasures taken.

Keywords: ISPS-Code, Wirtschaftliche Auswirkungen der Hafen- und Schiffssicherheit, Sicherheit der Transportkette, Piraterie, Kriminalität, Terrorismus

1. Einleitung

Der 11. September 2001 hatte auf unterschiedliche Aspekte des täglichen Lebens Auswirkungen. Der Bestsellerautor Frederick Forsyth beschreibt in seinem Buch »Der Afghane« das Szenario eines Schiffsdiebstahls auf hoher See, bei dem ein gestohlenen Schiff als Waffe gegen das Kreuzfahrtschiff »Queen Mary II«, auf dem ein G8-Treffen stattfindet, eingesetzt werden soll. Dieses Szenario ist nicht allzu weit entfernt von der Nutzung entführter Flugzeuge als Angriffswaffe.

Diese etwas reißerische Annahme eines möglichen Anschlags verdeckt aber einige wahrscheinlichere Störungsmaßnahmen der internationalen Seeverkehrsströme. Über 90 Prozent des weltweiten Warenaustausches findet heute auf dem Seeweg statt. Nadelöhre wie der Suez-Kanal, der Panama-Kanal, der Nord-Ostsee-Kanal, das Bab el Mandeb, die Straße von Gibraltar oder die Straße von Malacca müssen hierbei passiert werden. Störungen »herkömmlicher« Art wie Unfälle, politisch bedingte Blockaden oder kriminelle Überfälle mussten immer einkalkuliert werden. Die terroristische Bedrohung der Seeverbindungen und des Schiffsverkehrs ist aber verhältnismäßig neu. Einen Anfang machte die Entführung des italienischen Kreuzfahrtschiffs »Archille Lauro« 1985. Palästinensische Terroristen wollten durch die Entführung des Schiffes und einiger nicht an Land gegangener Passagiere inhaftierte Terroristen freipressen. Das Schiff war dem Überfall wehrlos ausgesetzt. Eine Kontrolle der Passagiere oder Besatzungsmitglieder, ähnlich der im Flugverkehr hatte nicht stattgefunden. Konsequenzen aus der Entführung wurden nicht gezogen, wohl wegen des glimpflichen Ausgangs. Der gezielte Sprengstoffanschlag auf den Zerstörer »USS Cole« im Jahr 2000 im Hafen von Aden wurde ebenfalls noch nicht als grundsätzlich neue Bedrohung angesehen. Erst der Anschlag auf den französischen Tanker »Limburg« vor der jemenitischen Küste im Oktober 2002, also nach 9-11, rief die Risiken von terroristischen Anschlägen auf die Zivilschiffahrt ins Bewusstsein.

2. Reaktion: ISPS-Code

Die internationale Staatengemeinschaft reagierte durch die Implementierung des *International Ship and Port Facility Security Codes* (ISPS-Code). Um die notwendigen Zeitläufe der Schaffung internationalen Rechts zu verkürzen, wurde der ISPS-Code dem bereits bestehenden SOLAS-Abkommen als Kapitel XI angehängt. Dies verlangte von den Unterzeichnerstaaten eine Umsetzung in nationales Recht innerhalb von 18 Monaten. Damit war der 01. Juli 2004 Stichtag für die Umsetzung der Forderungen des ISPS-Codes in Bundesrecht.

2.1 Aufgaben der Hafenbetreiber im ISPS-Code

Der ISPS-Code verlangte von den Hafenanlagenbetreibern zum Teil erhebliche Umstrukturierungen ihrer Betriebe bzw. baulichen Aufwand. So hat nun jede Hafenanlage, die Frachtschiffe von mehr als 500 t BRZ und/oder Fahrgastschiffe abfertigt, die jeweils in internationaler Fahrt sind, Maßnahmen gemäß dem ISPS-Code zu treffen. Dazu gehörten u.a. die komplette Umfriedung der Anlage, die regelmäßige Schulung aller Mitarbeiter in Sicherheitsbelangen, die Sicherstellung von Zugangskontrollen und Kontrollen des Betriebsgeländes, die Einrichtung von »restricted areas« (Sicherung der für den Warenumschlag notwendigen Einrichtungen) und Stellung eines sicherheitsüberprüften Hafensicherheitsbeauftragten (PFSO) der alle geforderten Maßnahmen einleitet, durchführt und überwacht. Alles Maßnahmen, die einen erheblichen Kostenaufwand bedeuteten. Erstens, durch den baulichen Aufwand und Unterhaltungskosten, zweitens durch den organisatorischen Aufwand und die dadurch verursachten Zeitverluste, drittens durch den personellen Aufwand in Bezug auf Neueinstellungen bzw. Personalfreistellungen für Schulungszwecke.

Begegnet wurde und wird diesen Mehrkosten durch zusätzliche Abwicklungsgebühren. Die »Terminal Handling Charge«, die den Frachtkosten schon vorher zugerechnet waren, wurden durch sogenannte »Security Charges« ergänzt. Viele Hafenanlagenbetreiber setzen diese zusätzliche Gebühr auf

* Philip Buse ist Rechtsanwalt und Geschäftsführer des Verbands für Sicherheit in der Wirtschaft Norddeutschland e.V. (VSWN).

ca. \$ 9,00 pro abgefertigten Container fest. Ein Betrag, der bezüglich des Werts des betreffenden Containers häufig eine reine Marginalie bedeutet, aber auf den Gesamtumschlag an Containern bei einigen großen Hafenanlagen eine erhebliche Summe ergibt. Die durch den ISPS-Code notwendig gewordenen Maßnahmen haben in der zwischenzeitlichen Betrachtung auch noch andere, mittelbar positive wirtschaftliche Effekte hervorgebracht. Der Diebstahl von und aus Containern innerhalb der Hafenanlagen ist signifikant zurückgegangen. Auch der »Schwund« von Betriebsvermögen ist durch die nun erforderlichen Kontrollen des Hafenbetriebsgeländes erheblich geringer geworden. Diese positiven Nebeneffekte waren in der ursprünglichen Kostenkalkulation regelmäßig nicht enthalten, sie sind allerdings auf Grund der mangelnden Vorhersehbarkeit auch kaum zu quantifizieren. Ein noch schwieriger zu quantifizierender, positiver Nebeneffekt sind die gesunkenen Rückführungskosten der Reedereien für blinde Passagiere. Durch die nunmehr weltweit mehr oder minder scharf durchgeführten Zugangs- und Betriebsgeländekontrollen ist es für illegale Einwanderer ungleich schwerer geworden, die Frachtschiffe zu erreichen, in deren Laderäumen sie sich verbergen können.

2.2 Behördenaufgaben im ISPS-Code

Von staatlicher Seite war die Schaffung einer neuen Behörde gefordert, die auf Grund der unterschiedlichen Staatsstrukturen im ISPS-Code als »*Designated Authority*« (DA) bezeichnet wird. Die DA analysierte die betreffenden Hafenanlagen und zeigte den Betreibern die erkannten Schwachstellen auf. Diese entwickeln einen individuellen Gefahrenabwehrplan, lassen ihn von der DA zertifizieren und treffen die erforderlichen Maßnahmen. Nachdem das Gros der Hafenanlagen den Ansprüchen des ISPS-Codes gerecht geworden war, übernimmt die DA nun Überwachungsaufgaben. Bauliche, personelle und organisatorische Veränderungen im Hafenbetrieb müssen durch Änderungsmitteilungen des PFSO an die DA gemeldet und im jeweiligen Gefahrenabwehrplan ergänzt werden. Die DAs erheben für ihre Tätigkeit regelmäßig Verwaltungsgebühren.

2.3 Wirtschaftliche Effekte des ISPS-Code

Neue Hafenanlagen, die anfangs außer Acht gelassen wurden, mussten ebenfalls ISPS-Code konform zertifiziert werden. Dies betraf vor allem Häfen an Rhein und Donau, die von seegehenden Küstenmotorschiffen angelaufen werden. Denn anders als die Binnenschiffe unterliegen die Küstenmotorschiffe dem SOLAS-Abkommen und somit auch dem in dessen Kapitel XI geregelten ISPS-Code. Eine Aufgabe, die bis heute in den Bundesländern Hessen und Baden-Württemberg nicht abgeschlossen ist, obwohl auch dort Küstenmotorschiffe Häfen bedienen. Wie bereits beschrieben, ist die Implementierung des ISPS-Codes für die Hafenanlagenbetreiber mit zum Teil erheblichen Kosten verbunden, so dass sich hier möglicherweise unberechtigte Standortvorteile ergeben können.

Den Schiffseignern legt der ISPS-Code ebenfalls mehrere Erfordernisse auf. So müssen nunmehr alle am internationalen Seeverkehr teilnehmenden Schiffe eine erkennbare, dauerhafte Registrierung der International Maritime Organization (IMO) tragen. Diese IMO-Nummer begleitet ein Schiff nun vergleichbar einer Fahrgestellnummer von der Bauwerft bis zum Abwracken. Jedes dieser Schiffe muss einen Ship Security Officer (SSO) haben, der die Einhaltung aller Anforderungen des ISPS-Codes an das Schiff gewährleistet. Für die Besatzungen der Schiffe bedeuteten die neuen Sicherheitsregelungen z.B., dass der Landgang nur unter erschwerten Umständen möglich und die Betreuung durch Hafeneinrichtungen erschwert ist.

Schiffsausrüster müssen nunmehr mit erheblichem zeitlichem Vorlauf den Bedarf der Schiffe ermitteln und ihre Anlieferungen genauestens mit den Hafenanlagen abstimmen. Die hierdurch entstehenden Mehrkosten der Reedereien und Schiffseigner werden im Regelfall durch eine nach Zielhäfen gestaffelte eigene »Security Charge« pro Frachteinheit ausgeglichen.

Alle durch die Neuregelungen anfallenden Kosten und Gebühren führen letztendlich zu einer Erhöhung der Frachtraten und treffen im Endeffekt die Endverbraucher. Dies spielt bei hochpreisigen Gütern (High-Value-/Low-Volume-Goods) eine eher untergeordnete Rolle. Bei Gütern, deren Verfrachtung erst durch die transportierte Menge lohnt, kann der zusätzliche Kostenaufwand durchaus dafür entscheidend sein, ob sich diese Ware noch wirtschaftlich lohnend international vermarkten lässt.

3. Weitere Schutzmaßnahmen

Die zumindest europäische Vergleichbarkeit der angeordneten und durchgeführten Maßnahmen zur Absicherung der Hafenanlagen soll durch Kontrolltätigkeiten der DAs der europäischen Nachbarländer gewährleistet werden. So könnte z.B. die Hamburger DA eine Kontrolle in Barcelona, die Genueser DA eine Kontrolle in Marseille, die Rotterdamer DA eine Kontrolle in Hamburg durchführen. Vergleichbare Standards wären mit vergleichsweise geringem Aufwand umsetzbar.

3.1 Supply-Chain-Security: Wie wird die Ware außerhalb des Hafens gesichert?

Die vorstehend beschriebenen Maßnahmen sichern die Hafenanlagen selbst als notwendiger Warenumschlagbetrieb und die Frachtschiffe gegen die unbefugte oder kriminelle Nutzung im Rahmen dessen, was wirtschaftlich noch vertretbar und gesetzlich den privaten Betreibern erlaubt ist. Das hierbei nur eine relative Sicherheit erreichbar ist, dürfte verständlich sein. Ein viel größeres Problem liegt aber in der Sicherheit der Transportkette. Durch den International verbindlichen ISPS-Code ist z.B. der Container beim Packbetrieb, auf dem Straßen-, Schienen- und Binnenschiffstransport nicht vergleichbar gesichert. Sollte also der Container auf einem Autobahnrastplatz geknackt und manipuliert werden, ohne dass dies auffällt, ist durch relative Sicherheit in der Hafenanlage und auf dem

Schiff nichts gewonnen. Im Gegenteil kann sich sogar daraus, dass der Container doch eigentlich »sicher« transportiert und zwischengelagert worden ist, ein etwas laxerer Umgang am Ziel ergeben.

3.2 Staatliche Maßnahmen und Vorgaben

Die USA sind diesem Problem mit der *Customs-Trade Partnership against Terrorism* (CTPAT) begegnet. Die Wirtschaft innerhalb der USA verpflichtet sich, die Warenverpackung und den Warentransport nach staatlichen Vorgaben durchzuführen, z.B. durch sicherheitsüberprüfte Arbeitskräfte, durch Nutzung von vorgegebenen und überwachten Lagerplätzen sowie Einhaltung von bestimmten Quarantänefristen. Diese Regelung findet jedoch nur auf Wirtschaftsbeteiligte in den USA Anwendung.

Europa schuf als Pendant den *Authorized Economic Operator* (AEO) der am 11. Juni 2005 im Artikel 5a des Zollkodex den deutschen Status eines zugelassenen Wirtschaftsbeteiligten bekam. Dieser Status ermöglicht es den Unternehmen innerhalb der EU durch Anwendung eines vereinfachten Verfahrens Bewilligungen für Zollverfahren mit wirtschaftlichen Auswirkungen zu erhalten. Diese Standardisierung und Verständigung auf eine gemeinsame Vorgehensweise mit EU-weiter Geltung ist hinsichtlich der Zuverlässigkeit möglicher Versender und Transporteure von wachsender Bedeutung.

Den Status eines AEO erhalten nur die Betriebe, die bereit sind, an einer personellen Sicherheitsüberprüfung teilzunehmen, deren Zahlungsfähigkeit unzweifelhaft ist und denen keine Verstöße gegen einschlägige Rechtsnormen vorgehalten werden können. Darüber hinaus müssen diese Unternehmen unter Umständen gewisse Sicherheitsstandards nachweisen. Insbesondere müssen sie die Einhaltung der entsprechenden Zollvorschriften in der Vergangenheit nachweisen können, sowie eine »die geeignete Kontrolle der Geschäfts- und Beförderungsunterlagen ermöglichende, zufrieden stellende Buchführung« aufweisen.¹ Sofern alle notwendigen Dokumente eingereicht worden sind, wird der Status des AEO nach Bearbeitung durch das jeweils zuständige Hauptzollamt erteilt. Die EU strebt derzeit die internationale Anerkennung des AEO Status durch die Drittländer an, so dass eine weitere Absicherung der Lieferkette erreicht wird.

3.3 Maßnahmen der Wirtschaft

Der AEO ist allerdings nur ein Aspekt hinsichtlich der Absicherung der Lieferkette. Innerhalb der internationalen Normierung durch die ISO wurde bereits die ISO Norm 28000 implementiert, welche die abschließende Dokumentation der gesamten Transportkette zertifiziert und bei Nichtbeachtung Strafen für die betreffende Geschäftsleitung vorsieht. Im sogenannten Basel-II-Abkommen werden Maßnahmen zur Sicherung der Kreditwürdigkeiten und Bonitäten sowie Bewer-

tungen über die Leistungsfähigkeit einzelner Unternehmen vorgesehen. Die Versicherungswirtschaft zeigt ihren Kunden ein erhöhtes Kostenrisiko bei Nichtbeachtung der Third-Party-Liability-Klausel zur Haftung gegenüber Dritten in den USA, Europa oder mehreren asiatischen Ländern auf.

Als drittes Element kommt die *Transported Asset Protection Association* (TAPA) hinzu. Diese wurde 1997 in den USA gegründet, um der grenzüberschreitenden Kriminalität gegen hochwertige Frachtgüter zu begegnen. Hierzu entwickelte die TAPA Frachtsicherheitsanforderungen (FSR). Diese wurden durch die Sicherheitsspezialisten der »High Tech«-Unternehmen entwickelt, die als Mitgliedsunternehmen der TAPA ein vitales Interesse an der Sicherheit der verfrachteten Waren haben. Diese Anforderungen beschreiben den Mindestgrad notwendiger Sicherheitsstandards beim Transport hochwertiger Waren. Da sich die TAPA an ihre Mitgliedsunternehmen richtet, die regelmäßig Branchen angehören, die hoch- und höchstwertige Güter herstellen und transportieren ist eine allgemeine Anwendung auf den Warenstrom kaum möglich.

3.4 Zwischenstaatliche Abstimmung

Der Warenverkehr zwischen Europa und den USA ist in absehbarer Zeit verhältnismäßig gut geschützt durch C-TPAT auf US-Seite und dem Zusammenspiel aus AEO, ISO 28000 sowie die durch die Wirtschaft selbst entwickelten Abwehrmaßnahmen gegen die allgemeine Kriminalität, die sich auch gegen terroristische Aktionen anwenden lassen.

Die Regionen, welche derzeit über keine supranationalen Wirtschaftszusammenschlüsse oder staatliche Übereinkommen verfügen, sind ungleich schlechter aufgestellt. Die ASEAN Staaten verfügen nicht einmal ansatzweise über gemeinsame Wirtschaftssicherheitsabkommen. Als Ursprungsländer eines Großteils des internationalen Warenstromes ist es aber gerade hier notwendig, verbindliche Sicherheitsmindeststandards einzuführen, um den gestiegenen Sicherheitsanforderungen der Empfängerstaaten zu entsprechen. Gleiches gilt für die meisten afrikanischen Nationen und im weitesten Sinne auch für den indischen Subkontinent.

Die arabischen Staaten des Golf Cooperation Council (GCC), sowie die südamerikanischen Staaten des MERCOSUR beginnen mit der Implementierung von Sicherheitsmaßnahmen hinsichtlich wirtschaftlicher Belange, um den Sicherheitsanforderungen Europas und Nordamerikas entsprechen zu können, ohne dass es zu empfindlichen Zeitverzögerungen und somit Kostensteigerungen in der Transportabwicklung kommt.

3.5 Neue Lösungsansätze

Neuentwickelte Software kann möglicherweise helfen durch Nutzung statistisch erhobener Werte, Anomalien in z.B. der Containerverfrachtung aufzuzeigen, wie längere Standzeiten an ungewöhnlichen Orten, unnötige Umwege in den Frachtrouten, Abänderung der ursprünglichen Warenbegleitpapiere

¹ Für eine nähere Erläuterung wird die Lektüre des Dokuments TAXUD/2006/1450 vom 29.06.2007 empfohlen.

u.ä. verhindert werden können. Durch die rasche Übertragung der Warenbegleitpapiere ließen sich Abweichungen von der Normalität bereits zu einem Zeitpunkt erkennen, in denen der entsprechende Container den Ausgangshafen möglicherweise noch nicht verlassen hat. Am Empfängerhafen ließe sich dieser Container separieren und durch geeignete Röntgenanlagen oder Durchsuchungen überprüfen.

Zusätzlich hierzu ist der Einsatz technischer Aufzeichnungsgeräte innerhalb des Containers denkbar. Diese kleinen und technisch robusten Geräte zeichnen Lichteinfall durch z.B. das Öffnen von Containertüren, die reine Transportzeit, Veränderungen der relativen Luftfeuchtigkeit und der Temperaturen auf. Im Empfängerhafen oder jeder anderen Stelle der Transportkette ließen sich diese Aufzeichnungen auslesen und beim Auftauchen von Anomalien entsprechende Maßnahmen einleiten.

Die unglaubliche Vielfalt des internationalen Warenverkehrs lässt aber leider auch hier genügend Spielraum für Manipulationen durch technisch und organisatorisch versierte Gruppierungen.

4. Piraterie

Der internationale Seeverkehr muss aber noch einer weiteren Bedrohung begegnen, die zwar schon sein fast 3000 Jahren bekannt ist, aber dennoch auch in unseren modernen, vernetzten Zeiten einen erheblichen Tribut fordert: die Piraterie.

4.1 Begrifflichkeiten

Die häufigste Vorstellung von Piraten ist eine nostalgisch verbrämte, durch Literatur und Filme romantisierte. Doch letztlich ist die moderne Piraterie eine Straftat mit oftmals tödlichem Verlauf, die mit einem geschätzten wirtschaftlichen Schaden von jährlich drei Milliarden US-Dollar einhergeht.

Piraterie geschieht im seltensten Fall auf hoher See. Die logistischen Anforderungen an die Täter sind regelmäßig zu hoch. Es fehlen entsprechende Schiffe zum Attackieren, ausgebildete Nautiker zum Hochseemannavigieren, die technischen Voraussetzungen, das Zielschiff zu finden und nicht zuletzt die Basen, um diesen technischen und personellen Aufwand zu unterstützen und dauerhaft gegen die »Pirateriebekämpfer« wie nationale Behörden, aber auch internationale Seestreitkräfte betreiben zu können. Attacken finden daher meist dort statt, wo sich der Seeverkehr ohnehin bündeln muss, wie z.B. in Meerengen, in Küstennähe vor größeren Zielhäfen sowie in der Nähe von gut geeigneten Verstecken wie Inselgruppen. Dies macht die Einstufung als Piraterie zum Teil schwierig. Da diese Taten in den Hoheitsgewässern von Nationalstaaten begangen werden, sind sie statistisch häufig als bewaffneter Raub definiert, wie jeder an Land begangene Überfall auch. Piraterie im Sinne der UN findet statistisch außerhalb von Hoheitsgewässern statt. Erst in jüngerer Zeit hat hier ein Umdenken bezüglich der Kategorisierung stattgefunden.

4.2 Kriminelle Intentionen

Das Ziel der Piraten ist abhängig von ihren jeweiligen Möglichkeiten eher das an Bord befindliche Geld, als die transportierte Ware oder gar das Schiff selbst. Die Schiffe haben regelmäßig hohe Geldbeträge in US-Dollars bei sich, um Hafengebühren, Schleppernutzungen oder Lotsen zu bezahlen. Diese Summen in den Schiffstresoren sind ein vorrangiges Ziel. Hierzu überfallen die Piraten das ankernde, auf Reede liegende Schiff und zwingen unter Gewaltandrohung zur Herausgabe des Geldes. Eventuell werden auch die persönliche Habe der Seeleute oder elektronische Geräte geraubt. Hierbei kommt es verhältnismäßig häufig zu Gewalttaten gegen die Besatzung. Andere Gruppen von Piraten sind eher an Teilen des Schiffes selbst oder der Ladung interessiert. Diese Gruppen verfügen meist über Kopien der Ladelisten, die sie von Komplizen erhalten. Gleichzeitig benötigen diese Gruppen das notwendige Gerät zum Abtransport bzw. Löscheinrichtungen. Durch den hohen Organisationsgrad dieser Gruppen, ist es für die Besatzung des geenterten Schiffes immer dann gefährlich, wenn es für die Aktion keine Zeugen geben darf.

Der wöchentlich erscheinende Piracy-Report erwähnt drei Vorfälle von Piratenüberfällen auf ankernde Schiffe in dem Zeitraum 29.09.-03.10.2007, bei denen entweder Schiffsbestände gestohlen oder Container geknackt wurden. Drei weitere Vorfälle im gleichen Zeitraum beschreiben Piratenaktionen gegen fahrende Schiffe, die von den Besatzungen abgewehrt werden konnten. Da es ungleich schwerer ist ein fahrendes Schiff zu entern als ein vor Anker liegendes, sind die Piratengruppen die derartige Aktionen durchführen spezialisierter, meistens bewaffnet und regelmäßig skrupelloser in der Wahl ihrer Mittel. Sie entern das Schiff meist in der Dunkelheit rauben in kürzestmöglicher Zeit die Vermögensgegenstände und verlassen das Schiff wieder, um in der näheren Umgebung zu verschwinden. Andere stoppen das Zielschiff durch Waffengewalt, sperren die Besatzung ein und nehmen sich mehr Zeit für ihren Raubzug. Eine Zeitbegrenzung bildet die durchschnittliche Eingreifzeit der möglicherweise zu Hilfe gerufenen staatlichen Stellen. Diese Vorgehensweisen erfordern eine Investition in Boote, Waffen und seemännisch geschultes Personal sowie verlässliche Informationen über »geeignete« Zielschiffe.

Eine seltenere, aber für die Besatzung gefährlichere Variante ist die Entführung des ganzen Schiffes. Dies traf insbesondere Tankschiffe, die bereits raffinierte Treibstoffe transportierten, welcher sich auf den Schwarzmärkten leicht absetzen lässt. Hierbei dauert die Piratenaktion meist mehrere Tage an, bis das gekaperte Schiff seine Ladung in einem von den Piraten benannten Hafen gelöscht oder an ein anderes Schiff übergeben hat. Die mögliche Beutesumme ist naturgemäß erheblich höher, der eigene kriminelle Aufwand jedoch ebenfalls. Das mögliche Eingreifen von Behörden muss sehr viel stärker einkalkuliert werden. In einigen Fällen wird das geenterte Schiff, nachdem es seine Ladung verloren hat, nicht wieder freigelassen, sondern für weitere kriminelle Zwecke genutzt. Die Besatzung wird in diesen Fällen entweder auf See ausgesetzt oder ermordet. Ein Beispiel hierfür ist das Schicksal des Tankers *Petro Ranger* im April 1998 in der Straße von Malacca

unterwegs mit einer Ladung Diesel und Flugzeugturbinenkraftstoff. Der Tanker wurde von Piraten geentert, die Ladung im Golf von Thailand in andere Tankschiffe umgeladen und das Schiff umbenannt in *Wilby*, die Besatzung wurde auf hoher See ausgesetzt. Die Piraten fuhren das umbenannte Schiff nach Hainan, um neue Ladung aufzunehmen und präsentierten hierzu falsche Dokumente.

4.3 Abgrenzungsproblematik

Die beschriebenen Modi Operandi treffen überwiegend auf kriminelle, gewaltbereite Gruppierungen zu, deren Ziel auf den Zugewinn von Vermögenswerten zur Verbesserung der jeweiligen eigenen Lebenssituation gerichtet ist.

In anderen Fällen dient der Piratenüberfall der unmittelbaren Geldbeschaffung für weitergehende Aktionen. Besonders in Südostasien steigt die Anzahl von Entführungen von Schiffen mit anschließenden Lösegeldforderungen für die Freilassung von Besatzungsmitgliedern. Die entführten Schiffe sind meist kleineren Typs und es werden überwiegend die ranghöheren Besatzungsmitglieder als Geiseln genommen und gegen Lösegelder von 10.000 US\$ bis 200.000 US\$ je nach Rang der Geisel wieder freigelassen. Diese Aktionen, die eine landgestützte sichere Basis benötigen, werden überwiegend von sogenannten Befreiungskämpfern wie der »Free Aceh Movement« (FAM) u.ä. durchgeführt. Mit den erpressten Summen wird der Untergrundkampf gegen die entsprechenden Regierungskräfte mitfinanziert.

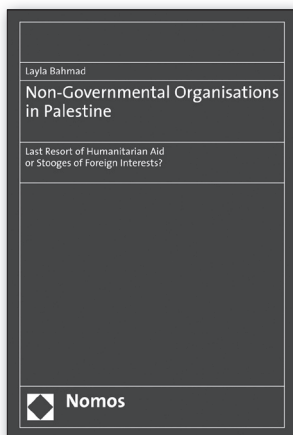
Die Grenze zwischen terroristisch geprägten Gruppierungen mit einer ideologischen Zielsetzung und rein vermögensorientierten, kriminellen Gruppen zu ziehen, ist schwierig. Die lange »Tradition« der Piraterie in Südostasien und die dezentrale Gliederung von terroristischen Gruppen in diesem Bereich

lässt die Grenzen von traditionell kriminellem und terroristischem Handeln verwischen. Abspaltungen von z.B. der Abu Sayaf Gruppe oder der Moro Islamic Liberation Front auf den Philippinen handeln nach außen hin im Namen ihrer Ideologie, nutzen jedoch die erpressten und erbeuteten Summen für persönliche Zwecke.

5. Fazit

Staatliche Reaktionen auf die Bedrohung sind zum einen der genannte ISPS-Code mit seinen Maßnahmen für die Schifffahrt, die Einführung multilateraler Seepatrouillen und die gesteigerte Überwachung der Meerengen aus der Luft. Dies schien einigen Erfolg zu bringen, da Anfang 2005 die Überfälle in der Straße von Malacca stark zurückgingen. Da sie aber zwischenzeitlich wieder angestiegen sind ist der Rückgang 2005 eher auf die Auswirkungen des Tsunamis Ende 2004 zurückzuführen. Mehr Erfolg verspricht hier das Programm Regional Cooperation Agreement on Anti-Piracy (ReCAAP), das den Aufbau von radargesteuerten Überwachungspunkten, den Ausbau von Marinesicherungskräften der Anliegerstaaten, sowie Aufklärungs- und Sozialprogramme für die verarmte Bevölkerung der anliegenden Küsten vorsieht.

Ob diese Maßnahmen greifen muss die Zukunft zeigen. Zwischenzeitlich bieten private Sicherheitsunternehmen den bewaffneten Schutz durch Sicherheitskräfte auf den Schiffen oder die Begleitung durch bewaffnete Boote oder Hubschrauber an. Dies stößt allerdings auf die Ablehnung der Anliegerstaaten, die bewaffnete Privatpatrouillen und Begleitungen in ihren Gewässern untersagen. Regelmäßig hat bisher die Bewaffnung der Handelsschiffe oder deren Besatzung zu einer »Aufrüstung« durch die Piraten geführt. Eine mögliche Steigerung der Gewalt und Brutalisierung der Piraterie ist sicherlich kein angestrebtes Ziel.



Non-Governmental Organisations in Palestine

Last Resort of Humanitarian Aid or Stoooges of Foreign Interests?

Von Layla Bahmad

2008, 295 S., broch., 49,- €, ISBN 978-3-8329-3393-7

Die Autorin liefert detaillierte Einblicke in die Arbeit und die Hintergründe von NGOs in Palästina. Demokratisch und islamisch orientierte NGOs konkurrieren um die Vergabe von westlichen Geldern. In dem Band wird untersucht, inwiefern dies islamistische Bewegungen fördert.

Bitte bestellen Sie bei Ihrer Buchhandlung oder bei Nomos |
Telefon 07221/2104-37 | Fax -43 | www.nomos.de | sabine.horn@nomos.de



Nomos