PiraT

Piraterie und maritimer Terrorismus als Herausforderungen für die Seehandelssicherheit: Indikatoren, Perzeptionen und Handlungsoptionen

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Thorsten Blecker / Thomas Will / Niclas Jepsen / Lutz Kretschmann / Andrea Resch

Analyse von schiffsbezogenen Sicherheitstechnologien zur Verzögerung von Angriffen im Kontext von Piraterie und maritimem Terrorismus

PiraT-Arbeitspapier zur Maritimen Sicherheit Nr. 10, August 2011

IFSH Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

TUHH Technische Universität Hamburg-Harburg

BUCERIUS LAW SCHOOL HOCHSCHULE FÜR RECHTSWISSENSCHAFT

DIW BERLIN

Institut für strategische Zukunftsanalysen der Carl-Friedrich von Weizsäcker Stiftung UG

Über die Autoren

Prof. Dr. Thorsten Blecker studierte Betriebswirtschaftslehre an der Universität Duisburg und promovierte 1998 dort. Er habilitierte 2004 an der Universität Klagenfurt in Österreich. In den Jahren 2004 und 2005 war er Gastprofessor für Produktion / Operations Management und Logistik an der Universität Klagenfurt, Österreich. Seit 2004 ist er Professor am Institut für Logistik und Unternehmensführung an der Technischen Universität Hamburg-Harburg. Zu seinen Forschungsschwerpunkten zählen folgende Themen: New Product Development & Supply Chain Design, Varianten- und Komplexitätsmanagement, Supply Chain Security, RFID, Decision Automation in Maritime Container Logistics and Air Cargo Transports. Außerdem ist er Leiter des Arbeitskreises Future Logistics, der sich mit Themen wie Compliance und Supply Chain Security auseinandersetzt.

Dipl.- Wirt.-Inf. Thomas Will studierte an der Universität Trier Wirtschaftsinformatik. Seit 2006 arbeitet er als Wissenschaftlicher Mitarbeiter an der Technischen Universität Hamburg-Harburg. Zu seinen Forschungsthemen zählen: Automatisierung in der Containerlogistik, Informationstechnologien in der Logistik, AutoID / RFID, Service-orientierte Architekturen, Multi-Agenten-Systeme, Anti-Terror-Compliance und Supply Chain Security.

Dipl.-Ing. oec. Niclas Jepsen studierte Wirtschaftsingenieurwesen an der Technischen Universität Hamburg-Harburg, der Universität Hamburg und der Hochschule für Angewandte Wissenschaften Hamburg. Seit 2010 arbeitet er als Wissenschaftlicher Mitarbeiter an der Technischen Universität Hamburg-Harburg. Zu seinen Forschungsthemen zählen u. a. Supply Chain Security, insbesondere Piraterie und maritimer Terrorismus.

Lutz Kretschmann studiert Wirtschaftsingenieurwesen an der Technischen Universität Hamburg-Harburg. Seine Interessenschwerpunkte liegen in den Bereichen Maritime Economics, Containerlogistik, Maritime Security, insbesondere Piraterie und maritimer Terrorismus.

Dipl.-Kffr. Andrea Resch studierte Betriebswirtschaftslehre an der Universität Regensburg. Seit 2009 arbeitet sie als Wissenschaftliche Mitarbeiterin an der Technischen Universität Hamburg-Harburg. Ihre Forschungsinteressen beinhalten u. a. Supply Chain Security Management und die sichere und effiziente Gestaltung von Logistikprozessen.

Impressum

Diese Arbeitspapierreihe wird im Rahmen des Verbundprojekts „Piraterie und maritimer Terrorismus als Herausforderungen für die Seehandelssicherheit: Indikatoren, Perzeptionen und Handlungsoptionen (PiraT)“ herausgegeben. Neben dem Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg (IFSH), das die Konsortialführung übernimmt, sind das Deutsche Institut für Wirtschaftsforschung (DIW), die Technische Universität Hamburg-Harburg (TUHH) sowie die Bucerius Law School (BLS) beteiligt; das Institut für strategische Zukunftsanalysen (ISZA) der Carl-Friedrich-von-Weizsäcker-Stiftung ist Unterauftragnehmer des IFSH. Das Projekt wird vom Bundesministerium für Bildung und Forschung (BMBF) im Rahmen des Forschungsprogramms für die zivile Sicherheit der Bundesregierung zur Bekanntmachung „Sicherung der Warenketten“ (www.sicherheitsforschungsprogramm.de) gefördert.

PiraT strebt ein Gesamtkonzept an, bei dem politikwissenschaftliche Risikoanalysen und technologische Sicherheitslösungen mit rechtlichen und wirtschaftlichen Lösungsvorschlägen verknüpft werden mit dem Ziel, ressortübergreifende staatliche Handlungsoptionen zur zivilen Stärkung der Seehandelssicherheit zu entwickeln.

Die „PiraT-Arbeitspapiere zu Maritimer Sicherheit/ PiraT-Working Papers on Maritime Security" erscheinen in unregelmäßiger Folge.

Allgemeine Anfragen sind zu richten an:
Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg (IFSH)
Dr. Patricia Schneider, Beim Schlump 83, D-20144 Hamburg
Tel.: (040) 866 077 - 0, Fax.: (040) 866 36 15, E-Mail: schneider@ifsh.de
Internet: www.ifsh.de und www.maritimesicherheit.eu

Inhaltliche Anfragen sind zu richten an:
Technische Universität Hamburg-Harburg (TUHH), Institut für Logistik und Unternehmensführung (LogU)
Prof. Dr. Thorsten Blecker, Schwarzenbergstraße 95 D, 21073 Hamburg
Tel: (040) 42878 3525, Fax: (01803) 55180 0956, E-Mail: blecker@ieee.org
Internet: www.logu.tu-harburg.de

Inhaltsverzeichnis

Executive Summary

In the past decade, maritime terrorism and piracy have become increasing threats for global sea trade. For instance, the number of only pirate attacks nearly doubled from 2005 to 2010. Additionally, the amounts of ransom paid increased up to seven digit ranges (USD) per case in 2010 and 2011. Furthermore, ships are potential targets for terrorist assaults with a potentially high impact. This is particularly shown by incidents like the suicide attack on the USS Cole in 2000 or the attack on the Limburg oil tanker in 2002.

In general, two strategies can be chosen in order to reduce the risk of maritime pirate or terrorist attacks: (1) evasion strategies like re-routing or (2) organizational, structural or technological changes in order to defend the ship in case of a potential attack.

The focus of this work will be on (2) technological changes. The investigation distinguishes between three different characteristics necessary to evaluate a ship's vulnerability: detection, delay and response. These physical protection system characteristics are used to classify the technologies. For that reason, the technological protection options are investigated and conceptualized within three connected working papers: the first paper contains detection technologies, the second one investigates delay technologies and the third one analyses response technologies.

The present working paper builds the second part of the above mentioned series on the technological protection of vessels.

The central objective of this paper is to present and evaluate physical protection technologies for ships that can **delay** pirate and terrorist attacks. A cost-benefit analysis is carried out for each technology and followed by a feasibility study. In addition to a theoretical analysis, expert opinions were obtained. This aims to identify both inapplicable technologies and those worthwhile further investigations. This paper (and the two corresponding papers) develops the basis for a concept to evaluate a vessel's vulnerability in regard to piracy and maritime terrorism by a number of indicators.

Abkürzungsverzeichnis

BSH	Bundesamt für Seeschifffahrt und Hydrographie
DIW	Deutsches Institut für Wirtschaftsforschung e.V.
DoD	(U.S.) Department of Defense
Ebd.	Ebenda
ICC	International Chamber of Commerce®
IFSH	Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg
IMB	International Maritime Bureau
MMWC	Merchant Maritime Warfare Centre
PPS	Physical Protection System
TUHH	Technische Universität Hamburg-Harburg
VDR	Verband Deutscher Reeder

Abbildungsverzeichnis

Tabellenverzeichnis

Vorbemerkung

Die Untersuchung von schiffsbezogenen Sicherheitstechnologien im Kontext von Piraterie und maritimem Terrorismus identifizierte über 40 Technologien und drei grundlegende Charakteristika, anhand derer die Sicherheitstechnologien klassifiziert werden können: Detektion, Verzögerung und Reaktion. Aufgrund des Umfangs und der Klassifizierung gliedert sich die Untersuchung in drei zusammenhängende Arbeitspapiere, die auf ähnlichen konzeptionellen und methodischen Grundlagen (Kapitel 1 und 2) basieren.

Das vorliegende Papier ist das Zweite in der Reihe von drei Arbeitspapieren, daher sollten sich Leser, die sich bereits mit dem ersten Arbeitspapier zur Detektion befasst haben, hauptsächlich den Kapiteln 3 und 4 widmen.

1 Einleitung

Die Bedrohung durch Piraterie und Terrorismus wächst.

In den letzten zehn Jahren stieg die Bedrohung durch Piraterie und maritime Terrorismus für den weltweiten Seehandel. Zum Beispiel verdoppelte sich die Anzahl der Angriffe durch Piraten allein in den Jahren zwischen 2005 und 2010 fast (International Chamber of Commerce International Maritime Bureau 2007, S.7; International Chamber of Commerce International Maritime Bureau 2011, S.6). Gleichzeitig stiegen die Lösegeldsummen pro Fall in 2010 und 2011 auf siebenstellige Beträge (Pelton 2011, S.1; Bowden 2010, S.9). Darüber hinaus stellen Schiffe potenzielle Ziele für terroristische Anschläge dar, deren Auswirkungen fatal sein können. Das zeigen auch Vorfälle wie die Angriffe auf die USS Cole im Jahr 2000 (U.S. Department of Defense 2001; GlobalSecurity.org 2011b, S.1) oder auf die Limburg in 2002 (GlobalSecurity.org 2011a, S.1; BBC News 2002, S.1).

Deutschland ist auf sichere Seewege angewiesen.

Gerade das Exportland Deutschland ist aufgrund seiner wirtschaftlichen Struktur auf sichere Seewege angewiesen (Flottenkommando 2010, S.4). Im Jahr der Wirtschaftskrise 2009 fiel der deutsche Export, ausgedrückt im Wert der ausgeführten Waren, um fast 18% (im Vergleich zum Vorjahr 2008) auf 808 Mrd. EUR und der Wert der importierten Güter sank um 16% (im Vergleich zu 2008) auf 674 Mrd. EUR. (Statistisches Bundesamt 2011, S.2) Trotz dieses massiven Einbruchs stieg der Anteil der auf dem Seeweg transportierten Waren um 1% auf 22,1%, wenngleich die Menge um 7,6% bzw. 15,97 Mio. t sank. (Flottenkommando 2010, S.96) Gleichzeitig steigt die Anzahl der Handelsschiffe unter deutscher Disposition stetig an. (Verband Deutscher Reeder 2011, S.22) Die mangelnde Präsenz polizeilicher und militärischer Kräfte in einigen Regionen der Weltmeere sowie das Wiedererstarken der weltweiten Piraterie(International Chamber of Commerce Commercial Crime Services 2011, S.1) und die Emergenz des maritimen Terrorismus[1] begründen bei Betroffenen den Wunsch nach verstärkten Sicherheitsmaßnahmen (Parfomak & Frittelli 2007, S.7) für Transporte durch die betroffenen Regionen, um finanzielle und personelle Schäden zu minimieren.

Technologien zum Schutz der Schiffe rücken in den Vordergrund.

Neben organisatorischen Maßnahmen, wie dem Umfahren gefährdeter Gebiete, und Schulungen des Personals zur Aufklärung über mögliche Gegenmaßnahmen zur Piraten- und Terrorismusabwehr, rücken technische Schutzmaßnahmen wie das Ausstatten der Schiffe mit verschiedenen Technologien und Gerätschaften derzeit in das Blickfeld der Betrachtung. (Brückner 2009, S.1-2)

Der Begriff Physical Protection System (PPS) beschreibt diese möglichen Maßnahmen bzw. Technologien zur Abwehr eines Angriffes auf ein Schiff und umfasst im Wesentlichen die folgenden drei Phasen: Detektion, Verzögerung und Reaktion. (Garcia 2006, S.2 ff.)

Das vorliegende Arbeitspapier konzentriert sich in der Analyse auf Technologien, die zur **Verzögerung** von Angriffen eingesetzt werden können.

[1] Zum Beispiel: Eine Suche in der RAND Database of Worldwide Terrorism Incidents http://www.rand.org/nsrd/projects/terrorism-incidents.html ergab am 09.04.2011 eine Summe von 136 Vorfällen weltweit, wo das Ziel(Target) des Angriffs als “Maritime” klassifiziert wurde.

Ziel des Arbeitspapiers ist die Identifikation und Analyse von Verzögerungstechnologien.

Das Ziel des vorliegenden Arbeitspapieres ist es, mögliche Technologien zur Verzögerung eines Angriffes auf ein Schiff zu identifizieren und in Bezug auf ihre Kosten, den möglichen Nutzen und die Realisierbarkeit zu analysieren. Darüber hinaus wurden die Ergebnisse der Analyse in einem Workshop, der am 29. März 2011 mit Experten aus den Bereichen Wirtschaft (Reeder, Versicherungen, Unternehmensberatungen, Anbieter von Sicherheitsdienstleistungen, Kapitäne, International Maritime Organization, International Chamber of Commerce), Schutzbehörden (Wasserschutzpolizei, Polizei, Bundeswehr, Bundeskriminalamt, Bundesamt für Seeschifffahrt und Hydrographie) und Wissenschaft (Recht, Friedensforschung und Sicherheitspolitik, Wirtschaftsforschung und Technik) durchgeführt wurden, validiert und erweitert. Sie sollen im Zusammenhang mit Nutzen bzw. Machbarkeit und Einsetzbarkeit der einzelnen Technologien erläutert werden.

Das Papier führt somit in einem ersten Schritt in das Konzept des Physical Protection Systems (Garcia 2007) ein und erläutert den Begriff der Verzögerung vor dem Hintergrund von Piraterie und maritimem Terrorismus. Das Konzept des Physical Protection Systems wird für Technologien zum Schutz von Schiffen gegen Angriffe auf See spezifiziert. Daran schließt sich ein Überblick über die Vorgehensweise bei der Bewertung von Kosten, Nutzen und Machbarkeit der einzelnen Technologien an. Weiter wird die Methode der Expertenbefragung und die Zusammensetzung der befragten Gruppen erklärt.

Im zweiten Schritt erklärt das Papier die im Rahmen der Untersuchung identifizierten Technologien, die auf Schiffen installiert werden können und zur Verzögerung von Angriffen dienen. Nach der Identifikation und Beschreibung werden diese Technologien nacheinander einer Kosten- und Nutzenbewertung unterzogen. Pro Technologie wird gleichzeitig die Machbarkeit der Technologie abgeschätzt und die Einsetzbarkeit mit den Ergebnissen aus der durchgeführten Expertenbefragung validiert.

In einem dritten und abschließenden Schritt fasst das Papier die identifizierten Technologien und ihre Bewertung im Bezug auf Kosten, Nutzen und Machbarkeit bzw. Einsatzfähigkeit zusammen. Das Ergebnis der Untersuchung mit dem Fokus auf Identifikation und Bewertung von Verzögerungstechnologien wird dargestellt. Im Anschluss erklärt das Papier die Probleme bei der Bewertung von terroristischen Bedrohungen. Abschließend wird der weitere Forschungsbedarf beschrieben.

2 Konzeptionelle und methodische Grundlagen

Der Begriff Verwundbarkeit und das Konzept des Physical Protection Systems werden erklärt.

Um ein Schiff optimal vor Angriffen durch Piraten oder Terroristen zu schützen, können verschieden Technologien eingesetzt werden. Zuerst erklärt das Papier die Verwundbarkeit (Vulnerabilität) im Zusammenhang mit dem Schutz von Schiffen vor Angriffen auf See. Danach stellt es ein Konzept zur Kategorisierung der Technologien zum Schutz des Objektes vor - das Konzept des Physical Protection Systems (PPS). (Garcia 2007) Im Anschluss daran wird die ausgewählte Funktion des PPS beschrieben: die Verzögerung. Später erfolgt eine Beschreibung der Expertenbefragungsmethode, die in dem vorliegenden Papier verwendet wird, um identifizierte Technologien bzw. der Einsetzbarkeit zum Schutz der Schiffe zu validieren. Zugleich erfolgt eine Begründung und Beschreibung der angewandten Szenariotechnik.

2.1 Vulnerabilität eines Objekts

Verwundbarkeit beschreibt hier die Schadensanfälligkeit von Schiffen gegenüber Piraten- oder Terroristenangriffen.

Die Vulnerabilität oder auch Verwundbarkeit beschreibt das „Maß für die anzunehmende Schadensanfälligkeit eines Schutzgutes in Bezug auf ein bestimmtes Ereignis“ (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe o. J., S.60). Im vorliegenden Papier wird das Objekt einem Schiff gleichgesetzt, das vor den Bedrohungen Piraterie und Terrorismus geschützt werden soll. Gerätschaften, die vor der Durchfahrt einer gefährlichen Passage am Schiff angebracht werden, können die Schadensanfälligkeit des Objektes (Schiff) senken. (Witherby Seamanship International Ltd. 2010, S.20 ff.) Die Vulnerabilität Deutschlands bezogen auf den Seehandel wurde bereits in Arbeitspapier 1 des Instituts für Friedensforschung und Sicherheitspolitik (IFSH) (Ehrhart u. a. 2010) und in Arbeitspapier 3 des Deutschen Instituts für Wirtschaftsforschung (DIW) (Engerer 2011) erläutert. Im Bezug auf die Sicherheit des maritimen Transportsystems konzentriert sich das vorliegende Papier auf den Schutz der Schiffe vor Angriffen durch Piraten oder Terroristen auf See.

2.2 Physical Protection System

Das PPS schützt das Objekt.

Die möglichen Maßnahmen zur Abwehr eines Angriffes können unter dem Begriff Physical Protection System (PPS) zusammengefasst werden. Die Aufgabe eines PPS ist die Gewährleistung der Sicherheit eines Objektes (im Sinne von Security). Dabei integriert es Menschen, Prozesse, elektronische und physische Komponenten zum Schutz des Objektes. (Garcia 2006, S.1) Bei den Objekten kann es sich um Personen, Eigentum, Informationen oder jede andere Form von Besitz dem ein Wert zugeschrieben wird handeln. (Garcia 2006, S.2) Das Ziel besteht darin, diese gegen offene oder verdeckte böswillige Handlungen zu schützen oder deren Durchführung im Vorfeld durch ein Abschrecken zu verhindern. Typische böswillige Handlungen, im Sinne von möglichen Bedrohungen für das Objekt, sind Sabotage von kritischem Equipment, Diebstahl von Eigentum oder Informationen sowie Verletzen von Menschen. (Garcia 2006, S.35) Im Kontext einer Risikobetrachtung bestimmt das PPS maßgeblich die Vulnerabilität des Objektes gegenüber diesen Bedrohungen. Ein PPS erfüllt folgende Funktionen: Abschreckung, Detektion, Verzögerung und Reaktion.

Das PPS erfüllt folgende Funktionen: Abschreckung, Detektion, Verzögerung und Reaktion.

Das Prinzip der Abschreckung beruht auf der Annahme, dass ein Angreifer sich aufgrund des äußeren Erscheinungsbildes eines Schiffes gegen einen Angriff entscheidet. Der Angriff muss - aus Sicht des Angreifers - mit einer zu geringen Aussicht auf Erfolg - im Verhältnis zum Aufwand - verbunden sein, sodass das Objekt zu einem unattraktiven Ziel wird. Technologien können so installiert werden, dass sie ausschließlich, teilweise oder keine abschreckende Wirkung haben.

Eine Abschreckungsfunktion ist nicht messbar.

Die Abschreckungswirkung der an einem Objekt installierten Sicherheitsmaßnahmen ist schwer zu bestimmen, da sie maßgeblich von der Entschlossenheit des Angreifers abhängt, trotz vorhandener Sicherheitsmaßnahmen einen Angriff durchzuführen. (Garcia 2007, S.2)

Detektion kann genutzt werden, um eine Reaktion einzuleiten.

Detektion bezeichnet das Erkennen eines unerlaubten Eindringens einer Person, eines Fahrzeuges oder eines Gegenstandes in einen geschützten Bereich durch eine Aufsichtsperson, die autorisiert ist eine angemessene Reaktion zu initiieren (Garcia 2007, S.83). Das System zu Detektion besteht grundsätzlich aus vier unterschiedlichen Elementen: (1) einem Erkennen des Eindringens, (2) einer Alarmbewertung, (3) einem Eingangskontrollsystem und (4) einem Detektions-Kommunikationssystems. Das erste Subsystem erkennt ein Eindringen und löst einen Alarm aus. Ein Eindringen muss nicht zwangsläufig in eine Bedrohung resultieren, so kann z.B. ein externer Sensor von einem Tier oder einem passierenden Objekt stimuliert werden. Die zuverlässigste Methode den Versuch eines Eindringens zu detektieren ist der Einsatz von Sensoren. Es kann jedoch auch von Wachpersonal oder Betriebspersonal übernommenen werden. (Garcia 2007, S.2) Nach der Auslösung eines Alarms evaluiert das zweite Subsystem, ob eine tatsächliche Bedrohung existiert und stellt ggf. Informationen über die Art der Bedrohung zur Verfügung. Je nach Ursache des Alarms wählt das Subsystem eine geeignete Reaktion aus. (Garcia 2007, S.127) Das Eingangskontrollsystems gewährleistet die Integrität des geschützten Bereichs durch die Begrenzung des Zugangs auf autorisierte Personen und die Überprüfung von ein- und ausgehenden Objekten auf z.B. Waffen oder Explosivstoffe bzw. auf Wertgegenstände oder Datenträger. (Garcia 2007, S.187) Das Detektions-Kommunikationssystem integriert alle anderen Subsysteme, aggregiert alle Informationen an einer zentralen Stelle und bereitet sie für den Nutzer auf, der - basierend auf den zur Verfügung gestellten Informationen – mögliche Reaktionen auf den Angriff einleitet und koordiniert.

Das vorliegende Papier konzentriert sich auf die Verzögerung.

Die dritte Funktion eines PPS ist die Verzögerung eines Angriffes, um mehr Zeit zur Verzögerung zur Verfügung zu haben und um den eingeleiteten Reaktionen die benötigte Zeit zur Entfaltung ihrer Wirkung zu geben (z.B. das Anfordern militärischer Unterstützung).

Verzögerung umfasst alle Elemente, welche das Eindringen eines Angreifers behindern.

Die Verzögerungsfunktion umfasst alle Elemente, welche das Eindringen eines Angreifers behindern und so die benötigte Zeit und den zu treibenden Aufwand des Eindringenden erhöhen. Durch das Verzögern des Angriffs wird die zur Verfügung stehende Zeit für eine Alarmbewertung und die Initiierung einer Reaktion erhöht. Im vorliegenden Papier wird Verzögerung unabhängig davon betrachtet, ob eine Detektion zuvor stattgefunden hat oder nicht. Typische Elemente eines PPS bestehen entweder aus strukturellen bzw. disponierbaren Barrieren, aus Technologien oder Gerätschaften, die am Schiff angebracht werden, oder aus Wachpersonal. (Garcia 2007,

S.220) Typische strukturelle Barrieren sind Zäune, Mauern, Stacheldraht, verstärkte Wände und Türen oder Fahrzeugsperren.

Innerhalb des vorliegenden Papiers werden nur Technologien bzw. Gerätschaften dem Physical Protection System zugeordnet, die vor der Durchfahrt einer gefährdeten Passage zusätzlich zur Standardausrüstung eines Schiffes angebracht werden.

Betrachtet wird nur Zusatzausrüstung.

Die vierte Funktion eines PPS ist die Reaktion auf einen Angriff. Sie impliziert ein weites Spektrum an Handlungsoptionen mit denen auf eine Sicherheitsverletzung reagiert werden kann. Eine angemessene Reaktion hängt von der Art der Bedrohung, den Konsequenzen eines erfolgreichen Angriffs, dem Wert des gesicherten Objektes, anderen Risikomanagementalternativen, die für das Objekt bestehen, dem Level an Risikotoleranz sowie rechtlichen Erwägungen ab. (Garcia 2007, S.237) Grundsätzlich kann eine Reaktion entweder unmittelbar und vor Ort oder nachträglich, d.h. verzögert erfolgen. (Garcia 2007, S.243) Eine unmittelbare Reaktion besteht in einem rechtzeitigen Aufbieten personeller, technologischer oder organisatorischer Sicherheitsmaßnahmen. Eine verzögerte Reaktion kann sinnvoll sein, wenn das Unterbinden des Angriffs weniger bedeutend ist, als ein Wiederaufnehmen des Betriebs, z.B. im Rahmen eines Notfallplanes. Beispiele für eine verzögerte Reaktion sind ein Durchsehen von Überwachungsvideos, Aufspüren und Zurückgewinnen von entwendeten Gütern oder eine strafrechtliche Verfolgung des Angreifers. (Garcia 2007, S.238)

Die vierte Funktion des PPS ist die Reaktion auf einen Angriff.

2.3 Verzögerung

Unter Verzögerung werden alle Bestandteile der Verzögerungsfunktion eines PPS zusammengefasst. Diese Bestandteile setzen sich aus strukturellen Barrieren, disponierbaren Barrieren und Wachpersonal zusammen. Die primäre Aufgabe dieser Komponenten ist, einen Angreifer auf dem Weg zum Ziel seines Angriffs zu verzögern oder wenn möglich, durch die Verzögerung von seinem Vorhaben abzubringen. Dadurch wird die Zeit zur Detektion sowie zur Umsetzung von Reaktionsmaßnahmen vergrößert. Maßnahmen, die verzögern, werden innerhalb des geschützten Bereiches angebracht, da sie nur so einen Einfluss auf die verfügbare Zeit zwischen Detektion und Reaktion haben können. Verzögerungstechnologien können auch wirken, wenn vor dem Einsatz dieser Technologien bzw. Gerätschaften noch keine Detektion des Angreifers stattgefunden hat. Zum Beispiel ist die Verzögerungswirkung von Nato-Draht völlig unabhängig davon, ob der Angreifer vorher entdeckt wurde, oder nicht. Als sekundärer Effekt geht von Verzögerungsmaßnahmen auch eine abschreckende Wirkung auf einen potentiellen Angreifer aus. Grundsätzlich ist die abschreckende Wirkung der Verzögerungsmaßnahmen und -technologien nicht direkt messbar und somit nur sehr schwierig zu bewerten.

Kernaufgabe der Verzögerung: verlangsamen oder vereiteln eines Angriffs.

Für die Verzögerung soll zwischen Ursprung der betrachteten Bedrohungen und der Vorgehensweise der Täter unterschieden werden. So haben, im Gegensatz zur Detektion, auch Motivation, Organisationsgrad und Grad der Gewaltanwendung des Angreifers einen Einfluss auf die Verzögerung.

Bei der Zuordnung von Maßnahmen zur Verzögerungs- oder Reaktionsfunktion kommt es im PPS Konzept zu Überschneidungen. So wird etwa Wachpersonal sowohl

der Verzögerung als auch der Reaktion zugeordnet. Um eine scharfe Abgrenzung der beiden Funktionen und eine Zuordnung von Maßnahmen zu den Funktionen zu ermöglichen, soll deshalb hier eine vom PPS Konzept abweichende Abgrenzung von Verzögerung und Reaktion vorgenommen werden.

Verzögerung setzt keine aktive Handlung der Besatzung voraus.

Zur Verzögerung tragen alle Maßnahmen an Bord des Schiffes und gegebenenfalls seiner Umgebung, sowie alle Eigenschaften des Schiffes bei, die einen Angreifer bei seinem Angriff verzögern, ohne dass sie eine aktive Handlung voraussetzen. Maßnahmen und Eigenschaften stellen die Verzögerungselemente des Schiffes dar. Diese Verzögerungselemente beschreiben welche Hindernissen, Herausforderungen und Schwierigkeiten der Angreifer auf dem Weg zu seinem Ziel bewältigen muss. Verzögerung ist auch ohne eine Detektion des Angriffs gegeben. Dies zählt jedoch nicht zur primären Funktion der Verzögerung.

Maßnahmen zur Verzögerung können nur an Bord des Schiffes oder in unmittelbarer Umgebung des Schiffes umgesetzt werden, da sich keine Maßnahmen auf dem offenen Meer, welches die Umgebung des Schiffes darstellt, implementieren lassen.

Die Ausprägung der Verzögerungselemente, die ein Schiff aufweist, hat neben der Verzögerung per se auch noch einen Einfluss auf ein Abschrecken eines Angriffes. Sind die Verzögerungselement für einen potentiellen Angreifer offen erkennbar, wird er sie in der, für seine Entscheidung für oder gegen einen Angriff maßgeblichen, subjektiven Erfolgswahrscheinlichkeit berücksichtigen. Ist die Wahrscheinlichkeit zu gering, wird er von einem Angriff absehen und sich, unter Umständen, auf ein weniger gut geschütztes Ziel konzentrieren.

Problematisch ist, dass weder die subjektive Erfolgswahrscheinlichkeit, noch der Einfluss, den bestimmte Verzögerungselemente auf diese haben, verlässlich zu ermitteln sind. Das gleiche gilt für die spezifische Ausprägung der Erfolgswahrscheinlichkeit, ab der von einem Angriff abgesehen wird. Das liegt daran, dass diese Ausprägung von den mit großer Unsicherheit behafteten Fähigkeiten und Intentionen der Angreifer abhängt.

Maßnahmen zur Verzögerung von latenten Bedrohungen werden nicht gesondert betrachtet. Im Moment der Detektion einer latenten Bedrohung wird diese zur evidenten Bedrohung und damit sind für beide Bedrohungen dieselben Verzögerungselemente relevant.

Die Verzögerungsfunktion bildet ab, in welchem Maß die Eigenschaften des Schiffes und die Maßnahmen, die an dem Schiff umgesetzt sind, in der Lage sind, das Vorankommen eines Angreifers zu verzögern bzw. zu behindern.

2.4 Kosten/Nutzen und Machbarkeit

Alle Technologien werden hinsichtlich ihrer Kosten, Nutzen und Machbarkeit untersucht. Diese Analysen ergeben zusammen eine Gesamtbewertung der einzelnen Technologien.

Die detaillierte Kostenanalyse der vorgestellten Sicherheitstechnologien erfolgte auf Basis von Herstellerinformationen und Expertenangaben. Die nachfolgende Tabelle veranschaulicht die betrachteten Kostenkomponenten und dient als Vorlage für alle folgenden Kostenanalysen. Es gelten folgende Definitionen:

Kosten-, Nutzen- und Machbarkeitsanalysen erfolgten auf der Basis von Hersteller- und Expertenangaben.

- Komponenten = wesentliche Bestandteile der Technologie
- Bezugseinheit = definiert die Bezugsgröße der Kosten (pro Schiff, pro Container, etc.)
- Investitionskosten = Kosten für die Erst-Ausrüstung einer Transporteinheit. Diese werden in Hardwarekosten, Softwarekosten und Schulungskosten unterteilt.
- Laufende Kosten = Kosten für den Betrieb dieser speziellen Technologie. Diese beinhalten Informationen zu Betriebskosten, Personalkosten, Wartungskosten und Entsorgungskosten soweit bekannt.
- Umrechnungskurs = USD 1.00 = 0.735601 EUR

Tabelle 1: Template Kostenanalyse

Technologie	Bezeichnung
Komponenten	
Bezugseinheit	Schiff oder Container
Investitionskosten	• Hardware • Software • Schulung
Laufende Kosten	• Betriebskosten • Personalkosten • Wartungskosten • Entsorgungskosten

Eine quantitative Bewertung des Nutzens von Technologien ist in vielen Fällen nur unzureichend möglich. Häufig sind die Kosten für die Wahrung von Sicherheit hoch, z.B. das Abschließen einer Lösegeldversicherung oder das Errichten von Abwehrsystemen. Falls es zu keinem Übergriff kommt, ist der Nutzen dieser Systeme neutral und eine quantitative Bewertung der Investition fällt negativ aus. Kommt es trotz getroffener technologischer Maßnahmen zu einem erfolgreichen Angriff, so ist der Nutzen in diesen Fällen ebenfalls nicht gegeben. Technologien können dennoch das Risiko eines Angriffs reduzieren, da sie die Wahrscheinlichkeit eines erfolgreichen Angriffs beeinflussen. Da bereits die Eintrittswahrscheinlichkeit bzw. die Veränderung eines Angriffes nur äußerst unpräzise ermittelt werden kann, ist auch der Nutzen von Technologien nicht objektiv quantitativ messbar.

Eine quantitative Nutzenbewertung ist in vielen Fällen unmöglich.

Aus diesem Grund wird der Nutzen im ersten Schritt dieses Arbeitspaketes argumentativ bewertet. Die Basis für diese argumentative Diskussion sind einzelne Experteninterviews sowie der -workshop, Literaturrecherche und Erfahrungen aus der Anwendung von bereits existierenden Technologien. Es soll gezeigt werden, ob die An-

Eine argumentative Nutzenbewertung wird durchgeführt.

wendung der jeweiligen Technik vorteilhaft oder nachteilig ist. Eine Technologie hat großen Nutzen, wenn die Sicherheit der Lieferkette oder die Sicherheit an Bord eines Schiffes durch sie erhöht werden kann. Auf diese Weise kann eine erste Bewertung vorgenommen werden, die bereits zum Ausschluss von einigen Technologien von der weiteren Betrachtung führen kann. Gleichzeitig ermöglicht eine argumentative Nutzenbewertung eine Auswahl von sinnvollen Technologien. Die Erkenntnisse der ersten Bewertung stellen die Grundlage der weiterführenden Nutzenanalyse dar.

Im zweiten Schritt folgen dann eine detaillierte Analyse und eine genaue Ausarbeitung des Nutzens. Um dies zu erleichtern, werden geeignete Methoden entwickelt, die die Bewertung strukturieren.

Die Analyse der Machbarkeit der einzelnen Technologien beinhaltet mehrere Aspekte. Diese sind z.B. Analysen der technischen Realisierbarkeit und der Praxistauglichkeit. Wenn eine Technologie bereits in den entsprechenden Bereichen angewendet wird, kann hierdurch beispielsweise auf eine Machbarkeit geschlossen werden.

Eine Technologie kann aus der technischen Perspektive betrachtet machbar sein und dennoch insgesamt als nicht machbar bewertet werden. Sollten den benötigten finanziellen Mittel zur Einführung einer Technologie kein angemessener Nutzen gegenüberstehen, so wird diese Technologie in der Praxis nicht realisierbar sein. Wenn eine Technologie noch nicht ausgereift ist und sich noch im Entwicklungsstadium befindet, ist eine Machbarkeit bzw. eine praktische Umsetzung zum aktuellen Zeitpunkt nicht gegeben. Für die Zukunft kann sich jedoch durchaus eine Machbarkeit ergeben. Technische Entwicklungen können jedoch nicht in jedem Fall vorhergesagt werden. Die Basis für die Machbarkeit der Technologien stellen wiederum Experteninterviews und -workshops, Literaturrecherche und Erfahrungen aus der Anwendung von anderen bereits existierenden Technologien.

Der Einsatz finanzieller Mittel spielt eine erhebliche Rolle bei der Bewertung der Technologien.

2.5 Expertenbefragung

Um die Eignung der identifizierten Technologien zu validieren und eventuell weitere Technologien zu identifizieren, wurde im Rahmen des Projektworkshops am 29. März 2011 eine Expertenbefragung durchgeführt.

Im Folgenden soll die verwendete Methode erläutert werden und die Zusammensetzung des Expertengremiums dargestellt werden.

Zur Validierung wurde eine Expertenbefragung im Rahmen des Pirat-Workshops im März 2011 durchgeführt.

Methode

Um eine Erweiterung der bisher identifizierten Technologien zuzulassen und zusätzliches Expertenwissen offen zu legen, wurden keine gänzlich strukturierten bzw. vordefinierten Interviews mit den Experten durchgeführt, sondern eine teilweise strukturierte Befragung. Die Experten erhielten zur Anregung der Diskussion vorab eine Liste der identifizierten Technologien.

Somit war die Expertenbefragung teilweise strukturiert, konnte aber durch die Beteiligten erweitert werden.

Methode: teilweise strukturierte Expertenbefragung.

Um Interaktionen zwischen einzelnen Experten zu ermöglichen, wurden Gruppenbefragungen durchgeführt.

Es wurden vier verschieden Szenarien vorab definiert:

Vier vordefinierte Szenarien wurden in einer Gruppendiskussion bearbeitet.

- Gruppe 1: Piratenangriff wird offensiv abgewehrt,
- Gruppe 2: Piratenangriff wird defensiv abgewehrt,
- Gruppe 3: Terroristischer Angriff wird offensiv abgewehrt,
- Gruppe 4: Terroristischer Angriff wird defensiv abgewehrt.

Die offensive Abwehr unterscheidet sich von der defensiven Abwehr dahingehend, dass in der offensiven Abwehr alle zur Verfügung stehenden Mittel verwendet werden sollen. In der defensiven Abwehr sollen nur die Mittel verwendet werden, deren Einsatz auch vor dem Hintergrund ethischer Gesichtspunkte geeignet und gerechtfertigt erscheint.

Die Experten waren aufgefordert, die Detektions-, Verzögerungs- und Reaktionstechnologien sowie deren Einsatz zum Schutz von Schiffen gegen Terrorismus und Piraterie, abhängig von den zugrunde gelegten Szenarien zu diskutieren.

Die Experten bewerteten die Technologien und präsentierten ihre Ergebnisse den Workshop-Teilnehmern.

Die Gruppendiskussion dauerte 50 Minuten. Im Anschluss daran wurden in 10 Minuten die Ergebnisse präsentiert.

Zusammensetzung der Gruppen

In den im Abschnitt „Methode“ aufgelisteten Gruppen befand sich jeweils ein neutraler Beobachter, der die Diskussion sowie deren Ergebnisse dokumentiert hat.

Der Beobachter forderte die Gruppen zu Beginn auf, pro Gruppe einen Sprecher festzulegen, der die Ergebnisse präsentiert.

Die Gruppen bestanden aus neun bis zehn Experten. Die Zusammensetzung innerhalb der einzelnen Gruppen wurde vorgegeben, um Heterogenität der Experten innerhalb der Gruppen sicherzustellen. Diese Heterogenität gewährleistet, dass es jeder Gruppe möglich ist, jede einzelne Technologie umfassend zu bewerten. Es befanden sich in jeder Gruppe Experten aus allen nachfolgend genannten Kategorien und - sofern möglich - aus allen Teilbereichen der drei Hauptkategorien:

Alle vier Gruppen waren im Vergleich zueinander homogen zusammengesetzt.

- Wissenschaft (Wirtschaftsforschung, Recht, Technologien, Friedensforschung und Sicherheitspolitik),
- Wirtschaft (Versicherungen, Unternehmensberatungen, International Maritime Organization IMO, Verband der Reeder, Kapitäne, Handelskammer ICC) und
- Schutzbehörden und andere Behörden (Polizei, Wasserschutzpolizei, Bundeskriminalamt BKA, Bundeswehr, Bundesamt für Seeschifffahrt und Hydrographie BSH).

Insgesamt waren 14 Experten aus der Hauptkategorie „Wissenschaft“, 15 Experten aus der Hauptkategorie „Wirtschaft“ und 10 Experten als Vertreter staatlicher Behörden beteiligt. Die durchschnittliche Teilnehmeranzahl pro Gruppe betrug gerun-

det 10 pro Gruppe, damit die Abstimmung innerhalb der Gruppe übersichtlich verbleibt.

In den einzelnen Gruppen herrschte Heterogenität. Um eine Vergleichbarkeit zwischen den vier Gruppen zu ermöglichen, waren die Gruppen relativ ähnlich in ihrer Zusammensetzung – also homogen im Vergleich untereinander. Beispielsweise wurde pro Gruppe darauf geachtet, dass Experten aus allen Teilbereichen involviert waren (Heterogenität) und dass die restlichen drei Gruppen zugleich ähnlich besetzt waren (Homogenität).

Ziel der Gruppendiskussion war die qualitative Beurteilung der identifizierten Technologien.

Die in der Gruppendiskussion hervorgebrachten Expertenmeinungen wurden dazu verwendet, die Technologien nach ihrer Eignung (qualitativ) zu beurteilen. Dies wird im folgenden Kapitel ergänzend zu der (quantitativ) oft sehr begrenzten Kosten- und Nutzenanalyse erläutert, so dass eine Gesamteinschätzung für jede Technologie vorgenommen werden kann. (Blumberg u. a. 2005, S.385 ff.)

Die Aufteilung in verschiedene Szenarien zeigt darüber hinaus, ob und in welchem Ausmaß Differenzen zwischen der Bedrohung durch maritimen Terrorismus und der Bedrohung durch maritime Piraterie bestehen. Zugleich legt die Bewertung der Experten Unterschiede zwischen offensiver und defensiver Perspektive offen.

Das Papier erläutert die in den Szenarien festgestellten Unterschiede in der nachfolgenden Diskussion der einzelnen Technologien ebenfalls, soweit diese festgestellt wurden.

3 Verzögerungstechnologien

Verzögerungstechnologien sollen Angreifern das An Bord kommen erschweren bzw. vereiteln.

Schiffsgebundene Maßnahmen und Technologien zur Verzögerung haben das Ziel das Schiff zu *härten.* Das bedeutet, dass die feindliche Annäherung und das An Bord kommen für Angreifer möglichst schwierig gestaltet wird bzw. verzögert oder gar vereitelt wird. Die Wirksamkeit der verwendeten Technologien ist unabhängig davon ob ein Angriff auf das Schiff bereits detektiert wurde oder nicht.

Die Kombination der Technologien und ihre Anordnung in Layer (Zwiebelprinzip) sind empfehlenswert.

Die ergriffenen Maßnahmen und eingesetzten Technologien werden in einem Schichtenkonzept (Zwiebelprinzip) angeordnet, bei dem sich die einzelnen Schichten gegenseitig stützen. (Brewer 2009, S.2 ff.) Ein Angreifer muss sich so hintereinander durch die einzelnen Lagen kämpfen und kann damit maximal in seinem Vorankommen verzögert werden.

Insgesamt wurden sechs verschiedene Technologien bzw. Gerätschaften identifiziert die als Verzögerungstechnologie kategorisiert werden können.

Die folgende Tabelle listet die Technologien, die im Rahmen des Projektes identifiziert wurden.

Tabelle 2: Übersicht über die Verzögerungstechnologien

Technologien zur Verzögerung eines Angriffes	
1. Schiffschrauben-Stopp	Vorrichtung um Taue oder Netze vom Schiff aus ins Wasser zu lassen. Ziel: Taue blockieren die Schiffsschrauben angreifender Boote.
2. Elektrozaun	Elektrozaun wird rund um die Reling angebracht. Ziel: Verhindern oder Verzögern des Enterns durch potenzielle Stromschläge.
3. Nato-Draht	Widerhakensperrdraht wird rund um die Reling angebracht. Ziel: Verzögerung des Enterns.
4. Water System	Leitungssystem mit Hochdruckdüsen. Ziel: Verhindern des Enterns, Verzögerung und Schutz des Schiffes durch Wasserstrahl.
5. Hot Water System	System mit Wärmetauscher, erhitzt Wasser zu heißem Sprühnebel. Ziel: Verhindern des Enterns, Verzögerung und Schutz des Schiffes durch Heißwasserstrahl.
6. Dummy Puppen	Keine Verzögerungstechnologie i. e. S. Ziel: Puppen täuschen höhere Mannschaftsstärke/-präsenz vor.

3.1 Schiffschrauben-Stopp

Um eine Verzögerung zu erreichen, können von der Reling abgelassene Taue die Schiffsschrauben angreifender Skiffs und Boote blockieren.

Grundsätzlich können Netze oder Taue, die rund um das Schiff zu Wasser gelassen werden, die Schrauben herannahender Schiffe zu blockieren. Umweltschützer verwenden solche „Prop foulers“ beispielsweise auch dazu, die Schrauben von Walfängern zu blockieren. (Animal Planet o. J.)

Schiffsschrauben-Stopp blockiert die Schiffsschrauben der Angreifer.

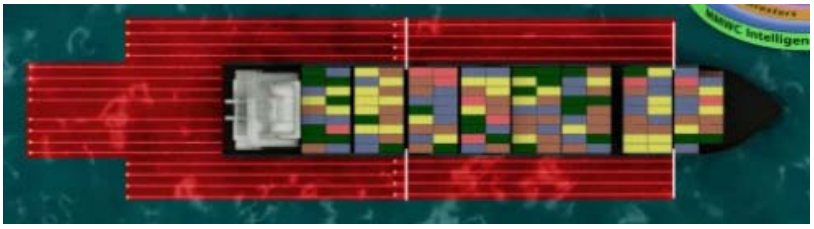
Zum Schiffsschrauben-Stopp existieren bereits Weiterentwicklungen. Zum Beispiel handelt es sich bei Propeller Arresters™ um ein von der Firma Merchant Maritime Warfare Centre (MMWC) entwickeltes Konzept, das die Schiffsschraube eines angreifenden Bootes blockiert. (Merchant Maritime Warfare Centre 2010a, S.1) In regelmäßigen Abständen werden dazu an der Reling des Schiffes Auslegebäume montiert, von denen Taue herabgelassen werden können.

Abbildung 1: Auslegevorrichtung und Rollen mit Propylenseilen*

**Quelle:* Merchant Maritime Warfare Centre o. J.*, http://www.mmwc.org/propeller_arresters.php#video.*

Weitere Taue werden am Heck des Schiffes angebracht. Sobald ein Seegebiet erreicht ist, in dem eine erhöhte Gefahr eines Angriffs besteht, werden die Taue heruntergelassen. Sie schwimmen auf der Wasseroberfläche und werden durch die Bewegung des Schiffes hinter diesem hergezogen. So entsteht ein geschützter Bereich um das Schiff herum.

Abbildung 2: Durch Propeller Arresters™ geschützter Bereich um ein Schiff*



**Quelle:* www.colreg.net.

Sobald das Boot eines Angreifers in diesen geschützten Bereich kommt, fährt es über eines der Taue. Das Tau wickelt sich um die Schiffsschraube, blockiert den Motor und setzt das Boot des Angreifers außer Gefecht.

Abbildung 3: Durch Propylenseile blockierte Schiffsschraube eines Skiffs*

**Quelle:* Merchant Maritime Warfare Centre, *http://www.mmwc.org/propeller_arresters.php#video.*

Auf diese Weise können auch mehrere Boote, die an einem Angriff beteiligt sind, immobilisiert werden. Um zu verhindern, dass Angreifer die Taue nutzen, um an ihnen hochzuklettern und so das Schiff zu entern, ist jedes Tau mit einer Sollbruchstelle versehen. Diese gibt ab einer bestimmten Belastung nach und ein daran hochkletternder Angreifer fällt herunter.(Maritime Security Review 2010, S.2; Merchant Maritime Warfare Centre 2010a, S.1) Zur Härtung des Schiffes können auch konventionelle Netze entsprechend dem hier beschriebenen Konzept eingesetzt werden.

Kosten:

Tabelle 3: Schiffsschrauben-Stopp

Technologie	Schiffschrauben-Stopp
Komponenten	• schwimmfähige Propylenseile 100 m lang • und für das Propeller Arrester™ System: Bausatz für Auslegebäume (10 m)*
Bezugseinheit	• Schiff
Investitionskosten	• 7.400 EUR (USD 10.000) ** • Software nicht notwendig • evtl. Schulungskosten
Laufende Kosten	• Wartung der Seile und ggf. Austausch von Komponenten

**Quellen:* Merchant Maritime Warfare Centre 2010a; Merchant Maritime Warfare Centre 2010b.

***Komponenten für ein Schiff mit einer Schiffslänge von 200m.*

Nutzen:

Schiffsschrauben-Stopp-Systeme haben ein gutes Kosten-Nutzen-Verhältnis.

Taue und Netze stellen ein geeignetes Mittel zum Verzögern von Angriffen dar. Der Einsatz von Tauen und Auslegesystemen zum Stoppen der Schiffsschrauben ist noch nicht ausreichend erprobt. So schreibt das Magazin „The Motorship“, dass die Schiffsschraube der angreifenden Piraten in einer Demonstration des MMWC zwar von einem Tau blockiert wurde, das Skiff aber mit verringerter Geschwindigkeit weiterfahren konnte (The Motorship 2010, S.1). In jedem Fall haben die Taue und Netze

eine abschreckende Wirkung auf potentielle Angreifer und können die Zeit, die zur aktiven Abwehr zur Verfügung steht, erhöhen.

Machbarkeit und Eignung:

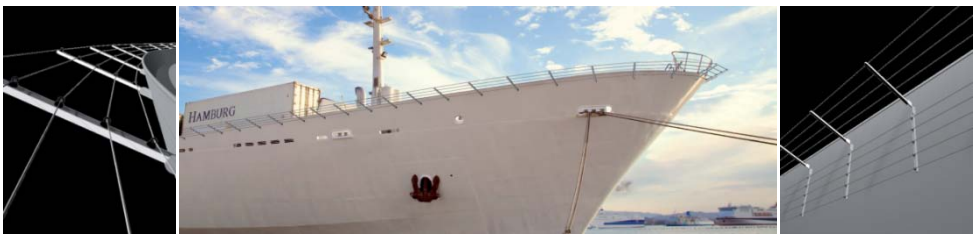
Konzepte zum Schiffsschrauben-Stopp existieren bereits. Der Investitionsaufwand und der Installationsaufwand sind eher gering. Ihre Machbarkeit ist somit praktisch bewiesen. Die im Workshop befragen Experten bewerteten den Einsatz des Schiffsschrauben-Stopp-Konzeptes wegen seines hervorragenden Kosten-Nutzen-Verhältnisses als sinnvoll und als Verzögerungstechnologie geeignet.

3.2 Elektrozaun

Elektrozäune können Angriffe verzögern.

Um ein Schiff gegen unbefugten Zutritt zu sichern, kann ein Elektrozaun in Höhe der Reling um das gesamte Schiff installiert werden. Der Zaun besteht aus mehreren blanken Drähten die in einer Führungskonstruktion in einem Winkel von 90° zur Schiffswand um das Schiff geführt werden. Je nach Bedrohungslage kann der Zaun abgeklappt werden, so dass er an der Schiffsreling anliegt und keine Behinderung darstellt bzw. Fluchtwege freigehalten werden. (Knott 2009, S.4; rotec GmbH 2011, S.1)

Abbildung 4: Elektrozaun in Höhe der Reling*



**Quelle:* rotec GmbH o. J., http://www.rotec-berlin.de/r_frames.htm?zaun/stromzaun/stromzaunfaqs.htm.

Der Zaun kann als Ganzes oder nur in einzelnen Abschnitten aktiviert werden. Dies ermöglicht es in Häfen nur die Steuerbord- oder Backbordseite zu schützen. Auch sieht das System Öffnungen vor, durch die etwa Lotsen an Bord kommen können, ohne den gesamten Zaun deaktivieren beziehungsweise demontieren zu müssen.

Berührungen führen zu starken Stromschlägen.

Ist der Zaun unter Spannung gesetzt, führt eine Berührung zu einem heftigen Stromschlag. Angreifer werden so dazu gebracht den Versuch das Schiff zu entern aufzugeben und von weiteren Versuchen abzusehen. Bei einer Spannung von 9.000 Volt ist der Stromschlag nicht tödlich und bleibt innerhalb des legalen Limits. (Knott 2009, S.4)

Der Elektrozaun kann neben der Verzögerungsfunktion auch eine Detektionsfunktion erfüllen.

Neben dem Abwehren eines Angriffes ist der Elektrozaun auch in der Lage einen Angriff zu detektieren. Sobald eine Berührung des Zaunes erfolgt, wird dieses durch die Kontrolleinheit des Systems erfasst und eine entsprechende Information über das Ereignis und den Zaunabschnitt, in dem es stattgefunden hat, generiert. Diese kann dazu genutzt werden einen Alarm auszulösen, um die Besatzung zu warnen, den Reeder oder zuständige Sicherheitsbehörden zu informieren oder andere Verteidigungsmaßnahmen zu initiieren. Für den Zaun sollen Warnschilder aufgestellt werden,

um die Abschreckungswirkung zu erhöhen. Zur Schiffsinnenseite sollte der Warnhinweis auf Englisch verfasst sein, zur Schiffsaußenseite in der Sprache der potentiellen Angreifer. (Witherby Seamanship International Ltd. 2010, S.29)

Der Einsatz eines Elektrozauns ist aufgrund der erhöhten Feuergefahr nicht empfohlen für Schiffe die Kohlenwasserstoffe[2] transportieren. (Witherby Seamanship International Ltd. 2010, S.28)

Kosten:

Tabelle 4: Elektrischer Zaun*

Technologie	Elektrischer Zaun
Komponenten	• Detektionseinheit • Energieeinheit • Elektrischer Zaun • Kontrollmodul • (Sirenen) • (Scheinwerfer)
Bezugseinheit	• Schiff
Investitionskosten	• Hardware • Software • Schulung
Laufende Kosten	• Nicht bekannt

**Quelle:* rotec GmbH 2010, S.3.

Es konnte kein Anbieter eines solchen elektrischen Zauns ermittelt werden. Aus diesem Grund können hier keine Kosten angegeben werden.

Nutzen:

Unbefugtes Betreten soll detektiert bzw. verzögert oder verhindert werden.

Obwohl ein Elektrozaun kein unüberwindbares Hindernis darstellt, kann er Angriffe deutlich verzögern bzw. verhindern. Zusätzlich besitzt er ein hohes Abschreckpotential gegenüber potentiellen Angreifern. (Sander 2008, S.1)

Machbarkeit und Eignung:

Die technische Machbarkeit ist gegeben. Der Einsatz eines Elektrozauns ist jedoch aufgrund der erhöhten Feuergefahr für Schiffe, die Kohlenwasserstoffe transportieren, nicht empfohlen. (Witherby Seamanship International Ltd. 2010, S.28) Die Installation und der Betrieb eines solchen Elektrozauns stellen einen erhöhten Aufwand dar.

Die Experten bewerteten Elektrozäune im Workshop als geeignet. Sie wiesen jedoch mehrfach darauf hin, dass der Zaun nur an einer einzigen Stelle von den Angreifern unterbrochen werden muss, um seine Wirksamkeit aufzuheben.

[2] wie beispielsweise Öle, die Kohlenwasserstoffe enthalten bzw. Kraftstoffe wie Erdöl, Benzin, Dieselkraftstoff oder Gase wie Methan, Ethan, Propan etc.

3.3 Nato-Draht

Stacheldraht ist ein verflochtener Draht, der in regelmäßigen Abständen mit Drahtspitzen oder Metallhaken versehen ist. (EDG Euro Draht Großhandel 2011, S.1) Gespannt oder in Rollen ausgelegt ist Stacheldraht ein effektives Hindernis das am Verlassen oder Betreten bestimmter Bereiche hindert.

Abbildung 5: Stacheldraht vs. Nato-Draht*

Stacheldraht **Nato-Draht**

**Quelle:* EDG Euro Draht Großhandel 2011, http://www.edg-koeln.de.

Weiteres Mittel zur Verzögerung ist das Anbringen von Nato-Draht entlang der Schiffsreling.

Nato-Draht ist eine Weiterentwicklung des Stacheldrahts. Bei diesem Draht wurden die eingewickelten Drahtstücke mit den scharfen Spitzen (Stachel) ersetzt durch scharfe Metallklingen. Nato-Draht ist zum Objektschutz wesentlich besser geeignet und hat den Stacheldraht weitgehend abgelöst. Die offizielle deutsche Bezeichnung für diesen Draht lautet „Widerhakensperrdraht“. Der hochfeste, innenliegende Drahtkern verhindert dabei das Trennen des Drahts mit einfachem Werkzeug. Die Metallklingen haben sowohl eine schneidende wie festhakende Funktion. Die Windungen des Nato-Drahtes sind untereinander mit sogenannten Verbindungsclips verpresst, was dem Draht ein röhrenförmiges Aussehen verleiht. (Euro Draht Großhandel 2011b, S.1)

Unbefugtes Betreten soll verhindert werden.

Zur Verteidigung gegen Angreifer wird der Draht, ähnlich wie bei Sicherheitszäunen im Objektschutz, als Übersteigschutz an der Reling befestigt. Der Nato-Draht verhindert mit seinen messerscharfen Klingen dadurch auf einfache Weise das unbefugte Betreten des Schiffes durch Angreifer. Eine weitere Möglichkeit ist das positionieren von Drahtrollen zum Versperren von Aufgängen, Öffnungen oder Durchgängen. Unabhängig davon wo auf dem Schiff der Draht Anwendung findet, ist es wichtig ihn gegen Aufnahme zu sichern. Bevor sich ein Schiff einem gefährdeten Gebiet nähert, wird der Nato-Draht an der Reling des Schiffes befestigt. Besteht kein Risiko eines Angriffs auf das Schiff, kann der Draht aufgerollt und verstaut werden. Ein Nachteil des Einsatzes von Nato-Draht ist die Verletzungsgefahr für die Besatzung bei ausgelegtem Draht und beim Auslegen selbst. Darüber hinaus muss der Draht auf den Schiffen bzw. im Hafen gelagert werden. (Knott 2009, S.4)

Kosten:
Nato-Draht bzw. Widerhakensperrdraht ist hat sehr viele Anwendungsmöglichkeiten, eine Rolle kostet ca. 60 Euro und umfasst ca. 8-10 Meter Draht (ausgezogen). Ein Meter (ausgezogen) kostet somit etwa zwischen 6 und 7,50 Euro.

Tabelle 5: Nato-Draht*

Technologie	Nato-Draht
Komponenten	• 30 Rollen Typ US Durchmesser 450 mm • 10 Rollen Typ US, Durchmesser 950 mm • 1 Rolle BS, Länge 200 mm • 2 Paar Spezialhandschuhe • 1 Verpackungseinheit C-Klammern (500 Stk.) • 1 Spezialzange
Bezugseinheit	• Schiff
Investitionskosten	• 1.100 EUR-1.500 EUR (USD 1.500 or USD 2.000) • 30 Rollen Typ US Durchmesser 450 mm á ca. 60 EUR pro Rolle = 1.800 EUR • 10 Rollen Typ US, Durchmesser 950 mm • 1 Rolle BS, Länge 200 mm • 2 Paar Spezialhandschuhe • 1 Verpackungseinheit C-Klammern (500 Stk.) • 1 Spezialzange • Keine Softwarekosten • Keine Schulungskosten
Laufende Kosten	• Keine laufenden Kosten

**Quellen:* Acher 2009, S.1-2; Euro Draht Großhandel 2011b, S.1.

Nutzen:

Ein Nato-Draht bietet für einen vergleichsweise geringen Aufwand einen gewissen Nutzen im Sinne einer Verzögerung und stellt zusätzlich eine Abschreckung dar. Im Falle eines Angriffs mit entsprechend starkem Werkzeug, kann dieser nicht durch einen Nato-Draht abgewehrt werden.

Machbarkeit und Eignung:

Nato-Draht hat ein sehr gutes Kosten-Nutzenverhältnis.

Ein Nato-Draht kann vergleichsweise einfach installiert und verwendet werden. Es ist keine technische Neuerung notwendig. Die Machbarkeit ist folglich gegeben. Die Expertenrunde bewertete den Einsatz von Stacheldraht als sehr sinnvoll. Zum Einen besteht beim Einsatz von Stacheldraht ein sehr gutes Kosten-Nutzen-Verhältnis, zum Anderen ist die Verzögerungswirkung bei Angriffen sehr gut und bereits erprobt.

Vor jeder Passage eines gefährdeten Gebietes muss der Draht neu verlegt werden.

Problematisch wurde nur die Tatsache bewertet, dass das Verlegen des Drahtes jedes Mal vor der Passage eines gefährdeten Gebietes vorgenommen werden muss und der Draht danach wieder abgenommen werden muss. Der Zeitaufwand hierfür ist abhängig von den Schiffsaußenmaßen. In diesem Zusammenhang wurde jedoch auch positiv bewertet, dass Stacheldraht sehr oft wiederverwendet werden kann. Die Experten bewerteten Widerhakensperrdraht bzw. Nato-Draht als geeignet für den Einsatz zum Verzögern von Angriffen auf See.

3.4 Water System

Das Water System verwendet Wasser zur Abwehr eines Angreifers. (Sander 2008, S.1-2) Ist das System dauerhaft eingeschaltet, ist es Teil der Verzögerung des Schiffes.

Angreifer werden mit Hochdruck-Wasser abgewehrt.

Beim Water System wird entlang der gesamten Reling des Schiffes ein Leitungsnetz verlegt an dem sich in regelmäßigen Abständen Hochdruckdüsen befinden. Ist das System aktiviert werden durch dieses Leitungsnetz große Mengen Meerwasser gepumpt und treten unter hohem Druck aus den Düsen aus. (Secure-Marine 2011b) Um die Wirksamkeit zu erhöhen können dem Wasser bei Bedarf Zusätze beigemischt werden, die etwa zu einer Reizung der Augen und Haut führen.

Der Wirkungseffekt des Systems besteht darin, dass

- ein Angreifer bei dem Versuch eines Enterns gegen die großen Mengen ausströmenden Wassers ankommen muss,
- die Sicht eines Angreifers eingeschränkt ist durch den austretenden Wassernebel. Dies hat sich in der Vergangenheit bereits als wirksam bei einer Abschreckung und Verzögerung von Piratenangriffen herausgestellt,[3]
- das austretende Wasser die Boote der Angreifer fluten bzw. die Schiffsmotoren oder elektrischen Anlagen an Bord beschädigen kann. (Witherby Seamanship International Ltd. 2010, S.31)

Als problematisch könnte sich die technische Lebensdauer dieser Technologie, vor allem die der Düsen, aufgrund der starken Beanspruchung durch Kontakt mit aggressivem Salzwasser erweisen.

Kosten:

Tabelle 6: Water System*

Technologie	Water System
Komponenten	• Wasserrohre/-leitung entlang der Bordkante (Stahl oder Hartgummi) • Hochdruckdüsen • Befestigungsklemmen • Wasserpumpe • IT-Kontrolleinheit
Bezugseinheit	• Schiff
Investitionskosten	• “medium cost“ • Installation durch Crew und Firmenvertreter
Laufende Kosten	• 1 Jahr Garantie auf alle Komponenten

[3] Witherby Seamanship International Ltd. (2010 : 31)

Technologie	Water System
Laufende Kosten	• Düsen müssen alle paar Stunden gereinigt werden um Verkrustung durch Salzwasser zu vermeiden • Keine Wasserkosten, da Seewasser ausreichend verfügbar

**Quellen:* (Secure-Marine 2011c; Secure-Marine 2011d)

Die Kosten für dieses System hängen im Detail von der Größe des zu schützenden Schiffs ab und können hier nicht angegeben werden.

Die Kosten hängen von der Größe des Schiffes ab.

Nutzen:

Ein Water System stellt ein nicht unerhebliches Hindernis für Angreifer dar.

Machbarkeit und Eignung:

Die Machbarkeit eines Water Systems ist vergleichbar mit der eines (im folgenden Abschnitt beschriebenen) Hot Water Systems. Anstelle von hohen Temperaturen, muss beim Water System hoher Druck erzeugt werden. Dies stellt jedoch keine hohen Voraussetzungen an die Technik. Kritisch ist hier jedoch wiederum der hohe Salzgehalt des Meerwassers.

Wie beim Hot Water System, bewerteten die befragten Experten die Technologie als geeignet, da auf vielen Schiffen bereits Wasseranlagen, die eigentlich zum Löschen von Bränden vorgesehen sind, installiert sind. Auch hier können diese Vorinstallationen genutzt und ausgebaut werden. Kombinationen mit abschreckenden Zusätzen wie beispielsweise Mittel, die die Schleimhäute reizen, wurden von den Experten ebenfalls wie bei den Hot Water Systems als Erweiterung vorgeschlagen.

Vorinstallierte Feuerlöschsysteme können zweckentfremdet werden.

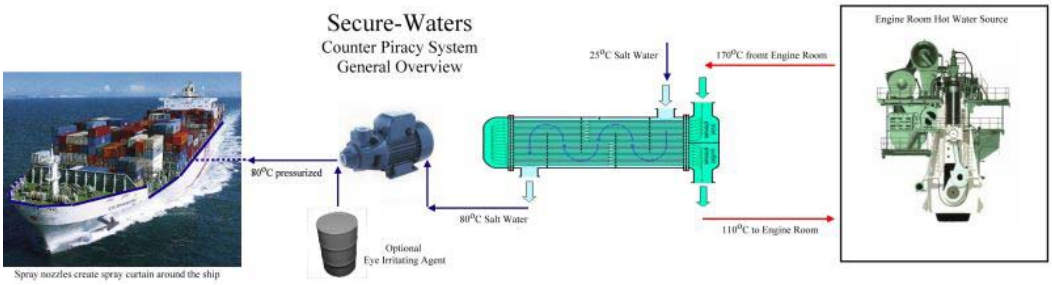
3.5 Hot Water System

Das Hot Water System setzt auf erhitztes Wasser, um einen Angreifer bei dem Versuch das Schiff zu entern zu behindern oder abzuwehren. Ist das System dauerhaft eingeschaltet ist es Teil der Verzögerung des Schiffes, wird es erst bei der Detektion eines Angriffes eingeschaltet ist es der Reaktion zuzuordnen.

Angreifer werden mit heißem Wasser abgewehrt.

Das System besteht aus einem Wärmetauscher mit dessen Hilfe heißes Wasser aus dem Maschinenraum genutzt wird um kaltes Meerwasser auf 80°C zu erhitzen. Das erhitzte Wasser wird von einer Pumpe in einem Netz von Leitungen entlang der Reling des Schiffes verteilt wo es aus speziellen Düsen als heißer Wassernebel austritt. (Secure-Marine 2011b) Um die Wirksamkeit zu erhöhen, können dem Wasser bei Bedarf Zusätze beigemischt werden, die etwa zu einer Reizung der Augen und Haut führen.

Abbildung 6: Hot Water System*



**Quelle:* Secure-Marine 2011c; Secure-Globe Pty Ltd.*

Der Wirkungseffekt des Systems besteht darin, dass

- der Kontakt mit dem heißen Wasser unangenehm bis schmerzhaft ist für einen Angreifer beim Erklimmen der Bordwand. Erhitztes Wasser hat sich in der Vergangenheit bereits als effektiv bei einer Abwehr von Piratenangriffen erwiesen(Witherby Seamanship International Ltd. 2010, S.32),
- die Sicht eines Angreifers eingeschränkt ist durch den austretenden Wassernebel. Auch dies hat sich in der Vergangenheit bereits als wirksam bei einer Abschreckung und Verzögerung von Piratenangriffen herausgestellt (Witherby Seamanship International Ltd. 2010, S.31),
- das austretende Wasser die Boote der Angreifer fluten bzw. die Schiffsmotoren oder elektrischen Anlagen an Bord beschädigen kann. (Knott 2009)

Kosten:

Tabelle 7: Hot Water System*

Technologie	Hot Water System
Komponenten	• Wasserrohre/-leitungen entlang der Bordkante (Stahl oder Hartgummi) • Niedrigdruckdüsen • Befestigungsklemmen • Wärmetauscher • Wasserpumpe • IT-Kontrolleinheit
Bezugseinheit	• Schiff
Investitionskosten	• „medium entry cost“ • „use for high-class shipping companies“ • Installation durch Crew und Firmenvertreter • Keine Softwarekosten • Schulung wird vom Anbieter durchgeführt
Laufende Kosten	• 1 Jahr Garantie auf alle Komponenten • Düsen müssen alle paar Stunden gereinigt werden um Verkrustung durch Salzwasser zu vermeiden • Seewasser ausreichend verfügbar

**Quelle:* Secure-Marine 2011c; Secure-Globe Pty Ltd.

Nutzen:

Als Problematisch könnte sich die technische Lebensdauer dieser Technologie, vor allem die der Düsen, erweisen aufgrund der starken Beanspruchung durch Kontakt mit aggressivem Salzwasser unter hohen Temperaturen. Außerdem ist fraglich, ob sich Angreifer von dieser Technologie dauerhaft davon abhalten lassen ein Schiff zu entern. Der Einsatz von einfachen Schutzanzügen auf Seiten der Angreifer würde die Wirksamkeit dieser Technologie bereits einschränken.

Machbarkeit und Eignung:

Die Machbarkeit ist ähnlich wie bei den Water Systems gegeben. Die Experten bewerteten Hot Water Systems als Verzögerungstechnologie geeignet, insbesondere wenn vorhandene Löschsysteme ohne großen Kostenmehraufwand genutzt werden können.

3.6 Dummy Puppen

Dummy Puppen können i. w. S. verzögernd wirken.

Um potentiellen Angreifern eine erhöhte Wachsamkeit der Besatzung sowie Bereitschaft zur Abwehr eines Angriffs zu signalisieren, können Dummy Puppen entlang der Reling oder auf den Aufbauten positioniert werden. (Witherby Seamanship International Ltd. 2010, S.22) Auch wenn Dummy Puppen für einen entschlossenen Angreifer keine Abschreckung darstellen dürften, können sie doch einen weniger zielstrebig vorgehenden Angreifer dazu bewegen, sich nach einem einfacheren Ziel umzusehen. Der Abschreckungs-Effekt kann nicht direkt nachgewiesen werden und fällt auch nicht in die Phase der Verzögerung. Die Wirksamkeit in der Phase der Verzögerung ist sehr begrenzt, denn beim Annähern wird der Angreifer ab einer gewissen Nähe zum Schiff feststellen können, dass es sich lediglich um eine Puppe handelt.

Abbildung 7: Dummy Puppe an der Reling*

**Quelle:* Witherby Seamanship International Ltd. 2010, S.22.

Um potentiellen Angreifern eine erhöhte Wachsamkeit der Besatzung sowie Bereitschaft zur Abwehr eines Angriffs zu signalisieren, können Dummy Puppen entlang der Reling oder auf den Aufbauten positioniert werden.

Kosten:

Tabelle 8: Dummy Puppen

Technologie	Dummy Puppen
Komponenten	• Dummy Puppe • Befestigungsmaterial
Bezugseinheit	• Schiff
Investitionskosten	• pro Dummy Puppe ab etwa 250 EUR • keine Softwarekosten • keine Schulungskosten
Laufende Kosten	• keine laufenden Kosten • keine Wartungskosten

Nutzen:

Auch wenn Dummy Puppen für einen entschlossenen Angreifer keine Abschreckung darstellen dürften, können sie doch einen weniger zielstrebig vorgehenden Angreifer dazu bewegen, sich nach einem einfacheren Ziel umzusehen. Insgesamt ist der Nutzen solcher Puppen jedoch vergleichbar gering.

Machbarkeit und Eignung:

Das Aufstellen von Dummy Puppen erfordert keine besonderen Kenntnisse. Da solche Puppen bereits existieren, ist die Machbarkeit gegeben. Im Expertenworkshop wurde der Einsatz von Dummy Puppen jedoch als ungeeignet bewertet. Zum Einen ist ihre abschreckende Wirkung innerhalb eines Angriffs nicht nachweisbar, zum Anderen können Angreifer ab einer gewissen Distanz erkennen, dass es sich lediglich um Puppen handelt.

Die Wirkung von Dummy Puppen ist nicht nachweisbar und auf eine Mindestdistanz der Angreifer begrenzt.

3.7 Maßnahmen zur Verzögerung

Der Vollständigkeit halber sollen hier, neben den Technologien auch die Maßnahmen genannt werden, die einen Angriff verzögern.

Typische Maßnahmen, die ergriffen werden können, sind:

- **Fahren mit der maximal möglichen Geschwindigkeit**. Damit wird dem Angreifer die Annäherung an das Schiff und auch das An Bord Kommen erschwert.
- **Entfernen aller Gerätschaften und Werkzeuge vom Deck des Schiffes.** Damit soll der Zugriff auf diese Gerätschaften und Werkzeuge durch die Angreifer verhindert werden.
- **Sichern und gegebenenfalls verschließen aller Türen und Luken die in das Innere des Schiffes führen.** Eine Evakuation, etwa im Brandfall, darf dadurch allerdings nicht behindert werden.
- **Sichern und gegebenenfalls verschließen aller Durchgänge und Aufgänge im Inneren des Schiffes.** Damit soll auch hier das Vorankommen eines Angreifers maximal erschwert werden. Auch hier muss eine Evakuation möglich bleiben.
- **Sichern und gegebenenfalls Blockieren der Nutzung aller Aufgänge und Leitern außerhalb des Schiffes**. Auch hier darf eine Evakuation nicht behindert werden.
- **Sichern und Verschließen aller Öffnungen in der Außenhaut des Schiffes** etwa auf dem Windendeck.
- **Sichern der Reling.** Wenn möglich sollten die gesamte Reling, aber insbesondere kritische Bereiche, gegen ein Entern mithilfe von Leitern oder Enterhaken gesichert werden. Hierbei können physische Barrieren eingesetzt werden. (Knott 2009, S.24-25,27,36)

Die Durchführung der Maßnahmen kann den Einsatz von Verzögerungstechnologien und -gerätschaften sinnvoll ergänzen.

Diese Maßnahmen können die vorgestellten Technologien ergänzen und wurden auch von den Experten empfohlen.

4 Fazit und Ausblick

4.1 Identifizierte Verzögerungstechnologien und deren Eignung

In einem ersten Schritt zur Analyse von Piraterie und maritimem Terrorismus wurden sicherheitstechnische Analysen durchgeführt. Innerhalb der Systematik eines Physical Protection Systems (PPS) wurden die Technologien entsprechend ihrer zeitlichen Abfolge in drei wesentliche Bereiche kategorisiert: Detektion, Verzögerung und Reaktion. Das vorliegende Arbeitspapier fokussiert die Kategorie Verzögerung. Die unterschiedlichen Sicherheitstechnologien wurden auf ihre Kosten, ihren Nutzen und ihre Machbarkeit hin analysiert.

Zur Schätzung der Kosten wurden mehrere Hersteller und auch Verwender befragt. Für den Schiffsschrauben-Stopp wurden beispielhafte Herstellerangaben ermittelt, die an die individuellen Gegebenheiten eines Schiffes angepasst werden müssen. Bei den Zäunen wie Elektrozaun und Nato-Draht lassen sich die Kosten pro Meter Schiffsreling ermitteln und umrechnen. Die Kosten für Dummy Puppen müssen lediglich mit der Stückzahl multipliziert werden. Leider konnten weder Verwender noch Hersteller konkrete Angaben zu den Kosten für (Hot) Water Systems machen, da diese sehr stark von den individuellen Eigenschaften der Schiffe abhängen auf denen sie implementiert werden sollen.

Die Kosten müssen an die individuellen Gegebenheiten der Schiffe angepasst werden.

Zur Bewertung von Nutzen und Machbarkeit wurde im Rahmen des Projektes PiraT ein Expertenworkshop durchgeführt. In dieser Expertenbefragung wurde mit Hilfe von Gruppendiskussionen und Szenariotechnik die Einsetzbarkeit und Eignung der identifizierten Technologien zur Bekämpfung von Piraterie und maritimen Terrorismus überprüft. Die Experten stellten fest, dass die folgenden Technologien bzw. Gerätschaften:

- Schiffsschrauben-Stopp,
- Nato-Draht,
- Elektrozaun,
- Water System und
- Hot Water System

zur Verzögerung eines Angriffes durch Piraten oder Terroristen auf See geeignet sind und empfahlen den Einsatz dieser Technologien. Die Befragten wiesen vermehrt darauf hin, dass besonders Elektrozäune sehr schnell unterbrochen werden können und dadurch funktionsunfähig gemacht werden können.

Sechs Technologien wurden identifiziert, davon wurden fünf von den Experten als zur Verzögerung geeignet bewertet und empfohlen.

Der Einsatz der von Dummy Puppen wurde von den Experten zwar als machbar eingeschätzt, aber nicht empfohlen, da sich die Bewertung des verzögernden Effektes von Dummy Puppen als schwierig herausstellte.

4.2 Probleme bei der Bewertung von terroristischen Bedrohungen

Im Workshop untersuchten die Experten zwei Szenarien aus dem Bereich der Piraterie und zwei Szenarien aus dem Bereich des maritimen Terrorismus.

Die Bedrohung durch maritimen Terrorismus ist schwieriger einzuschätzen als die Bedrohung durch Piraterie. Dies wirkt sich auch auf die Diskussion zum Einsatz von Technologien aus.

Sie stellten fest, dass die Bedrohung durch maritimen Terrorismus schwieriger zu bewerten ist und damit auch das Risiko nur äußerst unpräzise einzuschätzen ist. Da Piratenangriffe (zum Nachteil der Transporteure) laut ICC/IMB gehäuft und oft in ähnlicher Weise stattfinden, lassen sich Schlüsse über Vorgehensweise und Motivation der Piraten ableiten. Dies führt dazu, dass für Piraterie die Gefährdungslagen in unterschiedlichen Regionen relativ zuverlässig eingeschätzt werden können und eine Systematik für die Entwicklung von Schutzmaßnahmen angewandt werden kann. Für den Bereich des maritimen Terrorismus ist dies jedoch nicht möglich. Maritime Angriffe durch Terroristen sind laut Experten sehr heterogen was Planung, Vorgehensweise und Motivation betrifft. Die Motivation bei terroristischen Angriffen ist sehr unterschiedlich von der der Piraten (Lösegeld). Terroristen beabsichtigen i.d.R. einen großen Schaden bzw. eine große Aufmerksamkeit zu erzeugen. Hieraus ergibt sich eine örtliche Flexibilität, die Piraten oftmals nicht besitzen. Eine Bedrohung durch Terroristen ist somit weniger an Regionen als an weitere Faktoren gebunden. Solche Faktoren hängen stark von den Motiven der jeweiligen Terroristen ab und sind somit schwierig zu verallgemeinern. Zudem ist ebenfalls keine übliche Vorgehensweise von Terroristen ermittelbar wie dies für Piraten möglich ist. Eine allgemeine, unpräzise und allgegenwärtige Bedrohungslage durch Terroristen erschwert die Analyse über den Einsatz von Technologien zur Bekämpfung vom maritimen Terrorismus. Die Bedrohung durch Piraterie ist vergleichsweise schematisch und prägnant, was die Spezifikation des Physical Protection Systems erleichtert. (Petretto; Schneider)

4.3 Weiterer Forschungsbedarf

Für das gesamte Physical Protection System wurden, auf das Schiff bezogen, mehr als 40 Technologien identifiziert. Davon entfallen auf die Verzögerungsphase sechs Stück. Für die von den Experten als geeignet eingestuften Technologien wie beispielsweise Water Systems und Drahtbarrieren müssen Weiterentwicklungen und neue Einsatzmöglichkeiten in der Zukunft beobachtet werden.

Die Voraussetzungen müssen detailliert untersucht werden.

Die benötigten organisationalen, strukturellen, personellen und informationstechnologischen Voraussetzungen wurden in die Untersuchung nicht detailliert einbezogen, sie müssen ebenfalls noch im Detail erläutert werden.

Indikatoren müssen entwickelt werden.

Weiterer Forschungsbedarf besteht darüber hinaus in der Bildung geeigneter Indikatoren zur Bewertung des Risikos und der Vulnerabilität des Objekts Schiff bezogen auf Piraterie und Terrorismus, sowie der Wirksamkeit möglicher technologischer Gegenmaßnahmen. Die Ausprägung der Indikatoren sollte in Anlehnung an die Klassifizierung der Technologien (Detektion, Verzögerung und Reaktion) erfolgen. Jede dieser Ausprägungen betrachtet einen wesentlichen Teil der Bewertung. Da die einzelnen Ausprägungen sich gegenseitig beeinflussen können, können sich nicht ausschließlich losgelöst von einander betrachtet werden. Hierfür sollte somit eine geeignete zusammenfassende Betrachtung bzw. Bewertung entwickelt werden. Eine de-

taillierte Analyse ermöglicht ein differenziertes Darlegen von Vulnerabilitäten und somit auch das Identifizieren von geeigneten technologischen Gegenmaßnahmen.

Literaturverzeichnis

Acher, J., 2009. Barbed Wire - Low-Tech Defence Against Pirates. Available at: http://af.reuters.com/article/somaliaNews/idAFLU61339120090730 [Zugegriffen Mai 25, 2011].

Animal Planet, *Whale Wars: Prop Fouler: Video : Animal Planet* , Available at: http://animal.discovery.com/videos/whale-wars-prop-fouler.html [Zugegriffen August 10, 2011].

BBC News, 2002. BBC NEWS | Middle East | Craft „rammed" Yemen oil tanker. Available at: http://news.bbc.co.uk/2/hi/middle_east/2303363.stm [Zugegriffen August 3, 2011].

Blumberg, B., Cooper, D. & Schindler, P., 2005. *Business Research Methods*, McGraw-Hill Education.

Bowden, A., 2010. The Economic Costs of Maritime Piracy. *One Earth Future Foundation Working Paper*. Available at: http://oneearthfuture.org/images/imagefiles/Cost%20of%20Piracy%20Final%20Report.pdf [Zugegriffen Mai 4, 2011].

Brewer, C., 2009. Maritime Security & Counter-Piracy: Strategic Adaptations and Technological Options. *Journal of Energy Security (JES)*. Available at: http://www.ensec.org/index.php?option=com_content&view=article&id=188:maritime-security-aamp-counter-piracy-stragegic-adaptation-and-technological-options&catid=94:0409content&Itemid=342 [Zugegriffen März 20, 2011].

Brückner, F., 2009. Schifffahrt: Reeder rüsten massiv gegen Piraten auf. *Handelsblatt*, S.1-2.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, o. J. Methode für Risikoanalyse im Bevölkerungsschutz. Available at: http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Wissenschaftsforum/Bd8_Methode-Risikoanalyse-BS.pdf?__blob=publicationFile [Zugegriffen August 3, 2011].

EDG Euro Draht Großhandel, 2011. Stacheldraht. Available at: http://edg-koeln.de/front_content.php?client=1&lang=1&parent=10&idcat=119&idart=79 [Zugegriffen März 31, 2011].

Ehrhart, H.-G., Petretto, K. & Schneider, P., 2010. Security Governance als Rahmenkonzept für die Analyse vonPiraterie und maritimem Terrorismus. PiraT Arbeitspapier. Available at: www.maritimesicherheit.eu.

Engerer, H., 2011. Piraterie und maritimer Terrorismus– Entwicklung und Bedeutung des Seehandels –. PiraT Arbeitspapier. Available at: www.maritimesicherheit.eu.

Euro Draht Großhandel, 2011b. Widerhakensperrdraht. Available at: http://edg-koeln.de/front_content.php?idcat=32 [Zugegriffen Mai 25, 2011].

Flottenkommando, 2010. *Flottenkommando Jahresbericht 2010 Marine. Fakten und Zahlen zur maritimen Abhängigkeit der Bundesrepublik Deutschland*, Glücksburg: Flottenkommando Marine.

Garcia, M.L., 2007. *Design and Evaluation of Physical Protection Systems*, Amsterdam [u.a.]: Elsevier Butterworth-Heinemann.

Garcia, M.L., 2006. *Vulnerability assessment of physical protection systems*, Amsterdam [u.a.]: Elsevier Butterworth-Heinemann.

GlobalSecurity.org, 2011a. Limburg oil tanker attacked. Available at: http://www.globalsecurity.org/security/profiles/limburg_oil_tanker_attacked.htm [Zugegriffen August 3, 2011].

GlobalSecurity.org, 2011b. USS Cole bombing. Available at: http://www.globalsecurity.org/security/profiles/uss_cole_bombing.htm [Zugegriffen August 3, 2011].

rotec GmbH, Schutz von Marineflotten durch Stromzaun. Available at: http://www.rotec-berlin.de/r_frames.htm?zaun/stromzaun/stromzaunfaqs.htm [Zugegriffen August 10, 2011].

rotec GmbH, 2010. Stromzaun APS 3000 Marine. Available at: http://www.freilandsicherung.org/downloads/stromzaun_aps3000_marine.pdf [Zugegriffen März 31, 2011].

rotec GmbH, 2011. Stromzaun® APS 3000 Marine. Broschüre.

International Chamber of Commerce Commercial Crime Services, 2011. Hostage-taking at sea rises to record levels, says IMB. Available at: http://www.icc-ccs.org/news/429-hostage-taking-at-sea-rises-to-record-levels-says-imb [Zugegriffen Mai 23, 2011].

International Chamber of Commerce International Maritime Bureau, 2011. *PIRACY AND ARMED ROBBERY AGAINST SHIPS - ANNUAL REPORT - 1 January-31 December 2010*, Available at: http://www.simsl.com/Downloads/Piracy/IMBPiracyReport2010.pdf [Zugegriffen August 3, 2011].

International Chamber of Commerce International Maritime Bureau, 2007. *PIRACY AND ARMED ROBBERY AGAINST SHIPS - ANNUAL REPORT - 1 January-31 December 2006*,

Knott, J., 2009. Die Paradoxie moderner See-Piraterie: Ihre Gefahren und wie man sie reduzieren kann. Available at: http://www.reederei-nsb.com/_uploads/media/3517_Piraten_Download_D.pdf [Zugegriffen Mai 25, 2011].

Maritime Security Review, 2010. Anti-piracy demonstration 14th September 2010 | Maritime Security Review. Available at: http://www.marsecreview.com/?p=297 [Zugegriffen Mai 25, 2011].

Merchant Maritime Warfare Centre, 2010a. Propeller Arrester FAQs. Available at: http://www.mmwc.org/propeller_arrester_faqs.php [Zugegriffen November 16, 2010].

Merchant Maritime Warfare Centre, 2010b. Countermeasures Comparison Chart. Available at: http://www.mmwc.org/images/countermeasures_comparison_chart.gif [Zugegriffen Mai 25, 2011].

Merchant Maritime Warfare Centre, *Propeller Arresters*, Available at: http://www.mmwc.org/propeller_arresters.php#video [Zugegriffen August 10, 2011].

Parfomak, P.W. & Frittelli, J., 2007. *CRS Report for Congress - Maritime Security: Potential Terrorist Attacks amd Protection Priorities*.

Pelton, R.Y., 2011. Rich Returns for Somali Pirates Evading Capture in Gulf of Aden. *Bloomberg Businessweek*. http://www.businessweek.com/news/2011-05-13/rich-returns-for-somali-pirates-evading-capture-in-gulf-of-aden.html [Zugegriffen August 3, 2011].

Petretto, K., o. J.Diebstahl, Raub und erpresserische Geiselnahme im maritimen Raum. PiraT Arbeitspapier im Erscheinen.

Sander, R., 2008. Seeräuber-Schutz: Mit Höllenlärm gegen Piraten - Wissen | STERN.DE. http://www.stern.de/wissen/technik/seeraeuber-schutz-mit-hoellenlaerm-gegen-piraten-646261.html [Zugegriffen Mai 25, 2011].

Schneider, P., o. J. Maritimer Terrorismus: Tätergruppen und Anschlagstypen. PiraT Arbeitspapier im Erscheinen.

Secure-Marine, 2011b. Secure Ship. Available at: http://www.secure-marine.com/ship/Secure-Ship_brochure.pdf [Zugegriffen Mai 25, 2011].

Secure-Marine, 2011c. Secure-Waters Hot Water. Available at: http://www.secure-marine.com/secure_water_hot.shtml [Zugegriffen Mai 25, 2011].

Secure-Marine, 2011d. Secure-Waters Water Cannon. Available at: http://www.secure-marine.com/secure_water_cannon.shtml [Zugegriffen Mai 25, 2011].

Statistisches Bundesamt, 2011. Außenhandel - Gesamtentwicklung des deutschen Außenhandels ab 1950. http://www.destatis.de/jetspeed/portal/cms/Sites/destatis/Internet/DE/Content/Statistiken/Aussenhandel/Gesamtentwicklung/Tabellen/Content100/GesamtentwicklungAussenhandel.psml [Zugegriffen April 2, 2011].

The Motorship, 2010. Pirates foiled by propeller arrestor – and weather. Available at: http://www.motorship.com/features101/ships-equipment/pirates-foiled-by-propeller-arrestor-and-weather [Zugegriffen August 5, 2011].

U.S. Department of Defense, 2001. *DoD USS COLE Comission Report*.

Verband Deutscher Reeder, 2011. Daten der deutschen Seeschiffahrt Ausgabe 2011.

Witherby Seamanship International Ltd., 2010. BMP3 Best Management Practice 3. Piracy off the Coast of Somalia and Arabian Sea Area. Available at: http://www.mschoa.org/bmp3/Documents/BMP3%20Final_low.pdf [Zugegriffen Mai 25, 2011].

www.colreg.net, propeller-arresters.jpg (JPEG-Grafik, 493x134 Pixel). Available at: http://www.colreg.net/propeller-arresters.jpg [Zugegriffen August 10, 2011].