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

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Thorsten Blecker / Niclas Jepsen / Thomas Will /
Lutz Kretschmann

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

PiraT-Arbeitspapiere zur Maritimen Sicherheit Nr. 9, 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.-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.

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.

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

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

Piracy and maritime terrorism have a significant and increasing influence on worldwide shipping. The number of pirate attacks alone has almost doubled over the past years from 276 registered attacks in 2005 up to 445 in 2010. Furthermore, the increasing number of attacks is accompanied by increasing amounts of ransom. The average ransom paid to Somali pirates has grown from $150,000 in 2005 to $5.4 million in 2010. Both developments lead to a total ransom amount paid to Somali pirates in 2010 of approximately $238 million. In addition to the ransoms paid there are even more costs involved, i.e. those for insurance premiums, navy forces, technological protection systems. “Oceans Beyond Piracy” estimates annual total costs of piracy of $7 to $12 billion. The additional costs are primarily spent in order to reduce the risks involved in piracy, but they also focus on the risks of maritime terrorism. Risks can generally be managed by different approaches. Firstly, risks can be avoided or reduced e.g. by the adjustment of shipping routes to avoid dangerous hot spots. Secondly, risks can be transferred to insurance companies. A further option, decreasing the vessel’s vulnerability, will be examined in further detail. This again can be achieved by different approaches: structural changes, organisational changes, additional human resources, and technological protection systems.

This investigation distinguishes between three different characteristics necessary to evaluate a vessel’s vulnerability: (1) detection, (2) delay and (3) response. (1) Detection indicates the ability to detect an attack by pirates. (2) Delay specifies a vessel’s ability to delay or repel an attack which was not previously detected. This increases the time available to detect and respond to an attack. The ability to (3) respond to a pirate attack requires prior detection of the attack. An additional delay also increases the given time to respond to the attack. Hence, the three characteristics can benefit from each other. In combination, these indicators provide information about a vessel’s vulnerability. At the same time, these characteristics are used to classify technologies. However, this paper only deals with technologies that contribute to a vessel’s ability to detect attacks by pirates or terrorists. Further technologies dealing with delay and response will be analysed in subsequent papers.

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 investigating. In this paper, the basis for a concept to evaluate a vessel’s vulnerability in regard to piracy and maritime terrorism by a number of indicators will be developed. This composition enables a sophisticated analysis of the vessel’s vulnerability. Weaknesses and therefore areas for improvement can be determined by this method in further research.

Abkürzungsverzeichnis

AIS	Automatic Identification System
ETA	Estimated Time of Arrival
GHz	Gigahertz
GNSS	Global Navigation Satellite Systems
HFSWR	Hochfrequenz-Oberflächen-Radar
LRIT	Long Range Identification and Tracking
PANDA	Predictive Analysis for Naval Activities
PITAS	Pirate and Terrorist Aversion System
PPS	Physical Protection System
RFID	Radio Frequency Identification
SAR	Synthetic Aperture Radar
Sat	Satellite
SIMONE	Ship Infrared Monitoring, Observation and Navigation Equipment
SOLAS	International Convention for the Safety of Life at Sea
UAV	Unmanned Aerial Vehicles
UUV	Unmanned Undersea Vehicle
VTS	Vessel Tracking System

Abbildungs- und Tabellenverzeichnis

Abbildungen

Tabellen

1 Einleitung

Das Exportland Deutschland ist aufgrund seiner wirtschaftlichen Struktur auf sichere Seewege angewiesen. Die mangelnde Präsenz polizeilicher und militärischer Kräfte in einigen Regionen der Weltmeere sowie das Wiedererstarken der weltweiten Piraterie und die steigende Bedeutung des maritimen Terrorismus begründen bei Betroffenen den Wunsch nach verstärkten Sicherheitsmaßnahmen für Transporte durch die betroffenen Regionen, um finanzielle und personelle Schäden zu minimieren. Neben organisatorischen Maßnahmen, wie dem Umfahren gefährdeter Gebiete, und Schulungen des Personals zur Aufklärung über mögliche Gegenmaßnahmen, rücken technologische/infrastrukturelle Maßnahmen, wie das Ausstatten der Schiffe mit unterschiedlichen Technologien, derzeit verstärkt in den Fokus der Betrachtung.

Zurzeit findet ein Wiedererstarken der weltweiten Piraterie und Steigen der Bedeutung des maritimen Terrorismus statt, welches einen merklichen Einfluss auf die Seefahrt hat.

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.

Detektion eines Angriffs stellt einen Teil des Physical Protection System dar.

Das Ziel des vorliegenden Arbeitspapieres ist es, mögliche Technologien zur Detektion eines Angriffes auf ein Schiff in Bezug auf ihre Kosten, den möglichen Nutzen und die Realisierbarkeit der diskutierten Technologie zu analysieren. Darüber hinaus wurden die Ergebnisse der Analyse in einem Workshop, der am 29. März 2011 mit Experten u.a. aus den Bereichen Schifffahrt bzw. Reedereien, Wirtschaft, Recht, Versicherungen, Polizei, Bundeswehr, Bundeskriminalamt, Friedensforschung, Sicherheitspolitik durchgeführt wurde, eingebunden. Sie fließen in die Bewertungen der Kosten bzw. Machbarkeit der einzelnen Technologien mit ein.

Das vorliegende Arbeitspapier befasst sich also mit der Funktion der Detektion eines PPS Systems und analysiert dieses.

2 Konzeptionelle und methodische Grundlagen

Um ein Schiff besser vor Angriffen durch Piraten oder Terroristen zu schützen, können verschieden Technologien eingesetzt werden. Im Folgenden wird zuerst die Verwundbarkeit (Vulnerabilität) im Zusammenhang mit dem Schutz von Schiffen vor Angriffen auf See erklärt und dann ein Konzept zur Kategorisierung der Technologien zum Schutz des Objektes vorgestellt – das Konzept des Physical Protection Systems (PPS).[1] Danach wird die im vorliegenden Papier ausgewählte Funktion des PPS beschrieben: die Detektion. Im Anschluss daran erfolgt eine Beschreibung der Expertenbefragungsmethode, die in dem vorliegenden Papier verwendet wird, um identifizierte Technologien bzw. deren Einsetzbarkeit zum Schutz der Schiffe zu validieren. Zugleich erfolgt eine Begründung und Beschreibung der angewandten Szenariotechnik.

2.1 Vulnerabilität eines Objekts

Die Vulnerabilität oder auch Verwundbarkeit beschreibt das „Maß für die anzunehmende Schadensanfälligkeit eines Schutzgutes in Bezug auf ein bestimmtes Ereignis“[2]. Im vorliegenden Papier wird das Objekt einem Schiff gleichgesetzt, das vor Bedrohungen durch 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.[3] Die Vulnerabilität Deutschlands, bezogen auf den Seehandel, wurde bereits in Arbeitspapier 1 durch das Institut für Friedensforschung und Sicherheitspolitik und in Arbeitspapier 3 durch das Deutsche Institut für Wirtschaftsforschung erläutert. Im Bezug auf die Sicherheit des maritimen Transportsystems konzentriert sich das vorliegende Papier auf den Schutz vor Angriffen auf Schiffe durch Piraten oder Terroristen auf See.

2.2 Physical Protection System

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.[4] Bei den Objekten kann es sich um Personen, Eigentum, Informationen oder jede andere Form von Besitz, dem ein Wert zugeschrieben wird, handeln.[5] Ziel ist es, 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 Informa-

PPS integriert Menschen, Prozesse, elektronische und physische Komponenten zum Schutz des Objektes.

[1] Garcia, *Vulnerability assessment of physical protection systems*, 2.

[2] Bundesministerium für Bevölkerungsschutz und Katastrophenhilfe, „Methode für Risikoanalyse im Bevölkerungsschutz“, 60.

[3] Witherby Seamanship International Ltd, „BMP3 Best Management Practice 3 - Piracy off the Coast of Somalia and Arabian Sea Area“.

[4] Garcia, *Design and Evaluation of Physical Protection Systems*, 1.

[5] Garcia, *Vulnerability assessment of physical protection systems*, 2.

tionen sowie Verletzen von Menschen.[6] 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.

Ein 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, so dass das Objekt zu einem unattraktiven Ziel wird. Technologien können so installiert werden, dass sie ausschließlich, teilweise oder keine abschreckende Wirkung haben. Eine Überwachungskamera-Attrappe hätte beispielsweise nur eine abschreckende, eine Überwachungskamera eine teilweise und eine versteckte Überwachungskamera keine abschreckende Wirkung. 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.[7]

Die Abschreckungswirkung der an einem Objekt installierten Sicherheitsmaßnahmen ist schwer zu bestimmen.

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.[8] Das System zur 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 einer 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, da hierdurch menschliches Versagen ausgeschlossen werden kann. Es kann jedoch auch von Wachpersonal oder Betriebspersonal übernommenen werden.[9] 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.[10] 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.[11] 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.

Detektion bezeichnet das Erkennen eines unerlaubten Eindringens einer Person, eines Fahrzeuges oder eines Gegenstandes in einen geschützten Bereich.

[6] Ebd., 35.
[7] Garcia, *Design and Evaluation of Physical Protection Systems*, 2.
[8] Garcia, *Vulnerability assessment of physical protection systems*, 83.
[9] Ebd.
[10] Garcia, *Design and Evaluation of Physical Protection Systems*, 127.
[11] Ebd, 187.

Die dritte Funktion eines PPS ist die Verzögerung eines Angriffes, um den eingeleiteten Reaktionen die benötigte Zeit zur Entfaltung ihrer Wirkung zu geben (z.B. das Anfordern militärischer Unterstützung). 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. Einige Quellen gehen davon aus, dass eine Verzögerung nur dann gegeben ist, wenn ein Eindringen erkannt wurde. Im vorliegenden Papier wird Verzögerung unabhängig davon betrachtet, ob eine Detektion zuvor stattgefunden hat oder nicht. Eine Verzögerung geschieht somit auch ohne eine Detektion. Typische strukturelle Barrieren sind Zäune, Mauern, Stacheldraht, verstärkte Wände und Türen oder Fahrzeugsperren. Disponierbare Barrieren finden nur im Fall eines Angriffs Verwendung, wobei sich ihre Funktionsweise zwischen der Behinderung in der Fortbewegung (z.B. Gitter, rutschiger oder klebriger Schaum) und der Beeinträchtigung der Sinneswahrnehmung (z.B. Rauch, Reizgas oder Verdunkelung) unterscheidet.[12]

Die Verzögerungsfunktion umfasst alle Elemente, welche das Eindringen eines Angreifers behindern und so die benötigte Zeit und den zu treibenden Aufwand des Eindringenden erhöhen.

Die vierte Funktion eines PPS ist die Reaktion auf einen Angriff. Es besteht 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.[13] Grundsätzlich kann eine Reaktion entweder unmittelbar und vor Ort oder nachträglich, d.h. verzögerte erfolgen.[14] 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.[15]

Eine Reaktion stellt ein aktives Handeln nach der Detektion eines Angriffs dar.

2.3 Detektion

Detektion bezeichnet das Erkennen einer potentiellen Bedrohung, welche üblicherweise innerhalb eines Bereiches oder an der Grenze zu einem Bereich um das zu schützende Objekt stattfindet. Je früher eine Bedrohung identifiziert wird, desto mehr Zeit steht für eine Reaktion zur Verfügung, weshalb eine Detektion bereits an der Grenze des geschützten Bereiches erstrebenswert ist. Ein geschützter Bereich weist mindestens einen regulären Zugang auf, über den autorisierte Personen und Gegenstände zu dem Objekt bzw. in das Objekt gelangen.

Der Zeitpunkt der Detektion ist entscheidend für die Zeit zum Einleiten von Gegenmaßnahmen.

[12] Garcia, *Vulnerability assessment of physical protection systems*, 232.
[13] Ebd, 237.
[14] Garcia, *Design and Evaluation of Physical Protection Systems*, 243.
[15] Garcia, *Vulnerability assessment of physical protection systems*, 238.

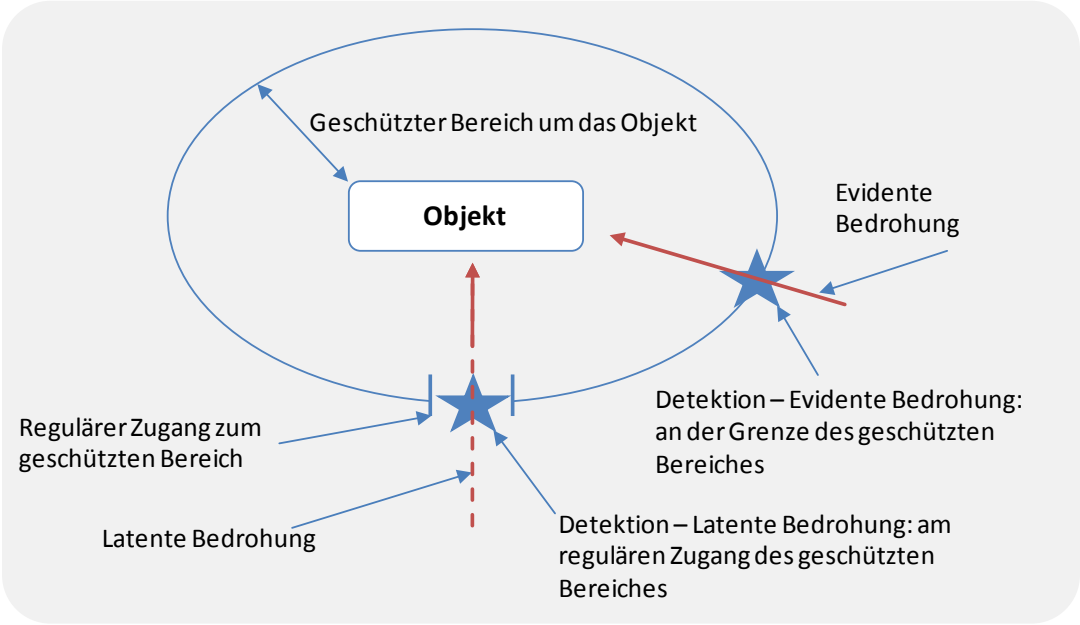
Bei einer Bedrohung wird grundsätzlich zwischen einer latenten, im Inneren eines Objektes zu Tage tretenden und einer evidenten, außerhalb des Objektes initialisierten Bedrohung unterschieden (vgl. Abbildung 1).

Bei einer **latenten Bedrohung** gelangt ein Objekt (z.B. eine Person, etwa ein Terrorist mit Sabotageabsichten oder ein Gegenstand, etwa eine Bombe) über den regulären Zugang in den geschützten Bereich unter Anwendung verschiedener Vorgehensweisen (z.B. unter Zuhilfenahme eines gefälschten Ausweises / getarnt als eine reguläre Postsendung). Erst nachdem sich das Objekt innerhalb des geschützten Bereiches befindet, legt es seine Tarnung ab und nimmt die konkrete Form einer Bedrohung an. Im optimalen Fall wird eine latente Bedrohung durch die regulären Zugangskontrollen entdeckt. Das „Eindringen" eines Terroristen mit einer Tarnidentität wird zwar detektiert, aber nicht als Bedrohung erkannt, solange die Tarnidentität aufrecht erhalten werden kann. Analog gilt dies z.B. für einen Container, der eine Bombe transportiert, jedoch aufgrund anders lautender Frachtpapiere eine „Tarnidentität" aufrecht erhält. Erst bei der Aufdeckung der wirklichen Identität durch das Objekt selber, oder durch Überprüfungen oder Zugangskontrollen, wird die Bedrohung offenkundig und somit **evident**.

Eine **evidente Bedrohung** bezeichnet Vorgehensweisen, die – sobald sie detektiert wurden – sich offenkundig als Bedrohung identifizieren lassen. Darunter fallen sowohl die Detektion eines unbemerkten verdeckten Vordringens durch den geschützten Bereich bis zum Objekt sowie ein offenes Vorgehen unter Ausnutzung von Schnelligkeit oder dem Einsatz von Gewalt. Die Fähigkeit der Detektion einer evidenten Bedrohung muss entlang der gesamten Grenze des geschützten Bereiches gegeben sein und auch den regulären Zugang umfassen.

Bei der Detektion evidenter Bedrohungen sollten die sich an der Grenze des geschützten Bereiches befindlichen Gebiete gemäß ihrer Eigenschaften differenziert werden. Befindet sich z.B. auf der einen Seite des Objektes ein dichter Wald und auf der anderen Seite das Meer hat dies sowohl Einfluss auf Annäherungsweise des Angreifers als auch auf die Möglichkeiten der Detektion. Eine Annäherung mit Fahrzeugen ist aus einem Waldgebiet kaum zu erwarten, jedoch ist eine visuelle Detektion eines Angreifers im Wald durch den starken Bewuchs erschwert. Eine Annäherung über das Meer ist sowohl über als auch unter Wasser möglich, wobei eine visuelle Detektion über Wasser schon in großer Entfernung möglich ist und unter Wasser nur mit zusätzlichen technischen Hilfsmitteln realisiert werden kann.

Abbildung 1: Geschützter Bereich und Detektion



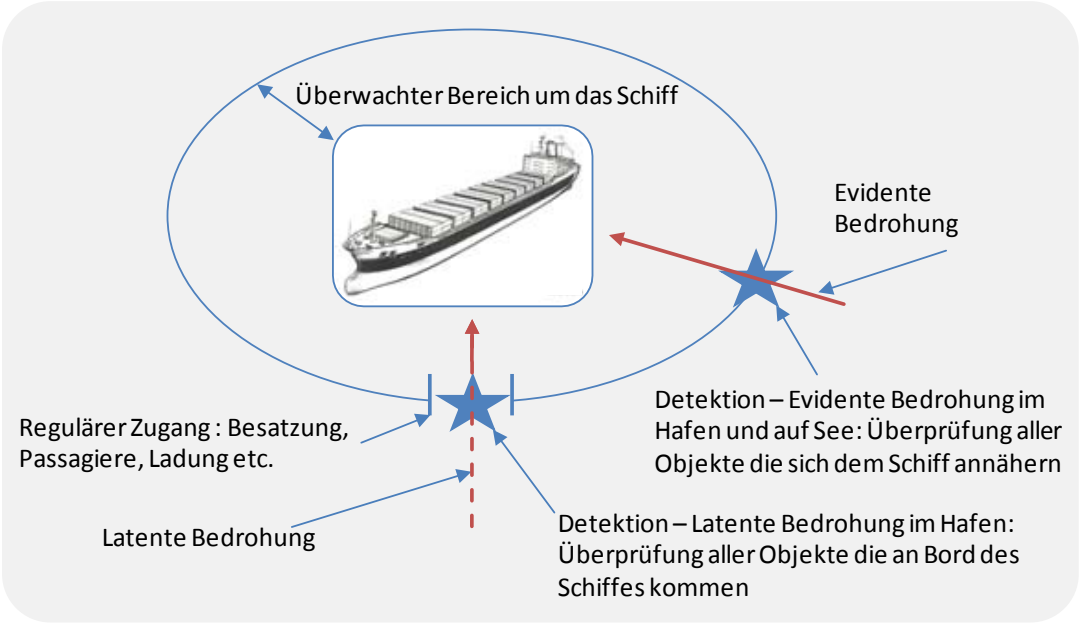
Der Bereich der Detektion muss ebenfalls das Umfeld des Schiffes umfassen.

Für ein Schiff ist die Abgrenzung eines geschützten Bereiches kritisch, da bauliche Maßnahmen außerhalb des eigentlichen Schiffskörpers zur Abgrenzung eines geschützten Bereichs problematisch sind. Eine Möglichkeit, einen geschützten Bereich abzugrenzen, ist, den geschützten Bereich auf den Schiffskörper zu beschränken und dort Detektionsmaßnahmen, wie etwa ein Netz von Sensoren, zu implementieren. Diese Detektion unmittelbar am Objekt ermöglicht es jedoch nicht, Verzögerung und Reaktion außerhalb des Schiffes zu realisieren. Ist das Ziel eines Angriffes das Erreichen des Schiffes, besteht so keine Möglichkeit einer Verzögerung oder Reaktion. Dies kann etwa bei einem terroristischen Angriff mit einer Bombe der Fall sein, die an einem Schiffskörper zur Explosion gebracht werden soll. Daher ist die Detektion auf das nähere und weitere Umfeld des Schiffes auszuweiten, indem alle – sich dem Schiff nähernden – Objekte erfasst und verfolgt werden, sobald sie sich innerhalb der Reichweite der Überwachung befinden. Das PPS soll ein Objekt somit in größtmöglicher Entfernung zum Schiff als potentielle evidente Bedrohung identifizieren und den Angriff so früh wie möglich verzögern, bzw. auf den Angriff reagieren (vgl. Abbildung 1).

Eine latente Bedrohung hingegen „nutzt“ den regulären Zugang zum Schiff. Dieser ist auf den Aufenthalt des Schiffes im Hafen beschränkt, wo Güter und Personen an Bord gelangen. In Ausnahmefällen kann es auch vorkommen, dass ein regulärer Zugang zum Schiff nicht auf den Aufenthalt im Hafen beschränkt ist (z.B. das an Bord Kommen von Lotsen oder der Küstenwache), welche als Sonderfälle aber nicht weiter untersucht werden. Als ein solcher Sonderfall gelten ebenfalls Schiffe, die auf Reede liegen. Für die Detektion der latenten Bedrohung sind alle Personen und Gegenstände, die an Bord des Schiffes gelangen, zu überprüfen. Die Überprüfung ist dabei nicht auf den unmittelbaren Übergang der Objekte an Bord begrenzt, sondern kann auch vorgelagert erfolgen. Bei einer vorgelagerten Überprüfung ist zu berücksichti-

gen, ob die Identität bzw. Integrität der Objekte zwischen Überprüfung und an Bord kommen sichergestellt ist.

Abbildung 2: Geschützter Bereich und Detektion – Schiff



2.4 Kosten / Nutzen / 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. Tabelle 1 veranschaulicht die betrachteten Kostenkomponenten und dient als Vorlage für alle folgenden Kostenanalysen. Es gelten folgende Definitionen:

- 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 = US$1.00 = 0.735601€[16]

[16] Umrechnung.org, „Universal Currency Converter™ Results“. Eröffnungskurs 31.01.2011

Tabelle 1: Template Kostenanalyse

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

In einem ersten Schritt erfolgt eine quantitative Nutzenbewertung.

Eine quantitative Bewertung des Nutzens von Technologien ist in vielen Fällen nur eingeschränkt möglich. In vielen Fällen 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 können. Da aber bereits die Eintrittswahrscheinlichkeit bzw. die Veränderung dieser nur äußerst unpräzise ermittelt werden kann, ist auch der Nutzen von Technologien nicht objektiv quantitativ messbar.

Aus diesem Grund wird der Nutzen im ersten Schritt dieses Arbeitspaketes argumentativ bewertet. Die Basis für diese argumentative Diskussion sind Experteninterviews und -workshops, Literaturrecherche und Erfahrungen aus der Anwendung von bereits existierenden Technologien. Es soll gezeigt werden, ob die Anwendung 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 bereits eine erste Bewertung vorgenommen werden, die zum Ausschluss von einigen Technologien von der weiteren Betrachtung führen kann. Gleichzeitig ermöglicht eine argumentative Nutzenbewertung bereits 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 Machbarkeit setzt sich u.a. aus technischer Realisierbarkeit und Praxistauglichkeit zusammen.

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. Sollte den benötigten finan-

ziellen Mitteln 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 im Entwicklungsstadium befindet, ist eine Machbarkeit bzw. eine praktische Umsetzung zum momentanen 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 bilden wiederum Experteninterviews und -workshops, Literaturrecherche und Erfahrungen aus der Anwendung von anderen bereits existierenden 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 und die Zusammensetzung des Expertengremiums dargestellt werden.

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

Es wurden vier verschieden Szenarien vorab definiert:

- 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. Insbesondere bei 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 Gruppendiskussion dauerte 50 Minuten. Im Anschluss daran wurden in zehn Minuten die Ergebnisse präsentiert.

ZUSAMMENSETZUNG DER GRUPPEN

In den oben aufgelisteten Gruppen befand sich jeweils ein neutraler Beobachter, der die Diskussion sowie deren Ergebnisse dokumentiert hat.

Zu Beginn wurden die Gruppen aufgefordert, 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 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:

- Wissenschaft (Wirtschaftsforschung, Recht, Technologien, Friedensforschung und Sicherheitspolitik)
- Wirtschaft (Versicherungen, Unternehmensberatungen, Anbieter von Sicherheitsdienstleistungen, International Maritime Organization, Verband deutscher Reeder, Kapitäne, internationale Handelskammer)
- Schutzbehörden und andere Behörden (Bundespolizei, Wasserschutzpolizei, Bundeskriminalamt, Bundeswehr, Bundesamt für Seeschifffahrt und Hydrographie)

Insgesamt waren 14 Experten aus der Hauptkategorie „Wissenschaft“, 15 Experten aus der Hauptkategorie „Wirtschaft“ und zehn Experten als Vertreter staatlicher Behörden beteiligt. Die durchschnittliche Teilnehmeranzahl pro Gruppe betrug gerundet zehn pro Gruppe, damit der Abstimmungsprozess 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).

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.[17]

Die Unterscheidung in verschiedene Szenarien soll darüber hinaus zeigen, ob und in welchem Ausmaß Differenzen zwischen der Bedrohung durch maritimen Terrorismus und der Bedrohung durch maritime Piraterie in Hinblick auf u.a. die Detektion bestehen. Zugleich lassen sich aus der Bewertung der Experten Unterschiede zwischen einer offensiven und einer defensiven Perspektive herausarbeiten.

Die unterschiedlichen Ergebnisse aus der Verfolgung der unterschiedlichen Szenarien sollen in der nachfolgenden Diskussion der einzelnen Technologien ebenfalls erläutert werden, soweit sie festgestellt wurden.

3 Detektionstechnologien

Detektionstechnologien ermöglichen bzw. unterstützen das Erkennen eines Angriffs bzw. eines Objektes, von dem potentiell eine Gefahr ausgeht. Dieser Abschnitt widmet sich schiffsgebundenen Systemen zur Unterstützung der Detektion von Angriffen.

Detektionstechnologien werden unterteilt in:

1. Schiffsgebundene Systeme zur automatischen Detektion eines Angriffs und
2. Bereichsüberwachung zur Erfassung potentieller Angreifer.
3. Schiffsgebundene Systeme zur Unterstützung der Detektion eines Angriffs,

Im Fall eines Angriffs auf ein Schiff ist es von großer Bedeutung diesen so früh wie möglich zu erkennen. Nur wenn dies gelingt, kann die Besatzung gewarnt, der Einsatz von schiffsgebundenen Verteidigungsmaßnahmen eingeleitet und eine Unterstützung durch Marine- oder andere Sicherheitskräfte veranlasst werden.

3.1 Schiffsgebundene Systeme zur Unterstützung der Detektion eines Angriffs

Schiffsgebundene Systeme zur Detektion von Angreifern unterstützen die Besatzung dabei, die Umgebung des Schiffes nach potentiellen Gefahren abzusuchen, und erhöhen so die Wahrscheinlichkeit, einen Angriff rechtzeitig zu erkennen. Sie ersetzen jedoch nicht eine Beobachtung der Umgebung des Schiffes durch die Besatzung selbst. Die Wachsamkeit sollte insbesondere in Seegebieten, für die ein erhöhtes Risiko bekannt ist, z.B. durch zusätzliche Ausgucker, verstärkt werden.[18]

Berichte zu erfolgreichen Entführungen lassen darauf schließen, dass nicht mehr als 15 bis 30 Minuten zwischen dem Beobachten verdächtiger Aktivitäten bis zu dem Entern vergehen.[19] Je mehr dieser Zeitraum vergrößert werden kann, desto größer ist die Chance, einen Angriff erfolgreich abzuwehren.[20]

[17] Blumberg, Cooper, und Schindler, *Business Research Methods*, 385ff.

[18] Witherby Seamanship International Ltd, „BMP3 Best Management Practice 3 - Piracy off the Coast of Somalia and Arabian Sea Area“, 21.

[19] Ploch u. a., „Piracy off the Horn of Africa“, 10.

[20] Knott, „The Paradox of Modern-day Piracy off Somalia: The dangers, and how to reduce them“.

3.1.1 Radar

Radarsysteme sind weitverbreitete Systeme zur Erfassung von Ort, Geschwindigkeit und Richtung von Objekten.

Radar ist ein Verfahren, das mithilfe von elektromagnetischen Wellen Objekte ortet und erkennt. Dazu werden von einem Transmitter elektromagnetische Wellen erzeugt, welche, wenn sie auf ein Objekt treffen, von diesem in Form eines Echos reflektiert werden. Nur ein kleiner Teil der ausgesendeten Strahlung wird reflektiert. Er bestimmt zusammen mit der Größe des Objekts das Radarecho. Nur wenn das Radarecho entsprechend groß ist, erkennt das Radar ein Objekt indem es die reflektierten Wellen mit einem Empfänger auffängt und auswertet.

Die Entfernung eines Objekts lässt sich anhand der Zeit, welche die Welle unterwegs ist, ermitteln. Die Richtung bestimmt sich über den Winkel der reflektierten Wellen und die relative Geschwindigkeit zum Radar kann anhand der Dopplerverschiebung des aufgefangenen Signals berechnet werden.[21]

Jedes Schiff ab einer Bruttoraumzahl größer 300 muss nach SOLAS Kapitel 5 mit einem 9 GHz Navigationsradar ausgestattet sein. Dieses ist darauf ausgelegt, Schiffsbewegungen in der Umgebung abzubilden, um dazu beizutragen, Kollisionen mit anderen Schiffen zu verhindern.[22] Problematisch im Zusammenhang mit dem Navigationsradar ist, dass kleine Seefahrzeuge, insbesondere bei hohem Seegang, nur unzureichend von dem Radar erfasst werden. Um dieses auszugleichen, sind kleine Seefahrzeuge mit einer Bruttoraumzahl kleiner 150 verpflichtet, einen Radarreflektor an Bord mitzuführen, der eine ausreichende Sichtbarkeit gewährleistet[23]. Es ist jedoch davon auszugehen, dass Boote von Piraten bzw. Terroristen dennoch keine Radarreflektoren verwenden.

Das Radar eines Schiffes sollte zu jedem Zeitpunkt besetzt sein, um eine Kollision zu vermeiden. Die dargestellten Radarsignaturen sollten dabei immer auch dahingehend geprüft werden, ob eine verdächtige Annäherung, die auf einen möglichen Angriff auf das Schiff hindeutet, zu identifizieren ist. Dies gilt insbesondere für Seegebiete, in denen bekanntermaßen eine erhöhte Gefahr eines Angriffes besteht.

KOSTEN

Tabelle 2: Radar (Hochfrequenz-Oberflächen-Radar)

Technologie	**Hochfrequenz-Oberflächen-Radar (HFSWR-Radar)**
Komponenten	• Radar
Bezugseinheit	• Schiff
Investitionskosten	• Hardwarekosten werden vom Hersteller (bspw. Raytheon[24]) nicht genannt • Softwarekosten nicht bekannt • Schulungskosten nicht bekannt
Laufende Kosten	• Nicht bekannt

[21] Issakov, *Microwave Circuits for 24 GHz Automotive Radar in Silicon-based Technologies*, 5.
[22] International Maritime Organization., *SOLAS*, 255.
[23] Amato u. a., „Fully solid state radar for vessel traffic services“, 2.
[24] Raytheon, „High Frequency Surface Wave Radar (HFSWR)“.

Die Kosten für ein HFSWR-Radar sind nicht bekannt, da die entsprechenden Hersteller keine Preisangaben veröffentlichen.

Tabelle 3: Radar (Synthetic Aperture Radar)

Technologie	Synthetic Aperture Radar (SAR)
Komponenten	• Radar
Bezugseinheit	• Schiff
Investitionskosten	• Hersteller wie z.B. Thales geben keine Information zu Investitionskosten und laufenden Kosten heraus → Schätzung eines Radarexperten: 2 - 10 Mio. $ (ca. 1,47 - 7,35 Mio.€) Stückpreis pro SAR inklusive Ersatzteile, Schulungen und Upgrades[25] • Softwarekosten nicht bekannt • Schulungskosten nicht bekannt
Laufende Kosten	• Nicht bekannt

NUTZEN

Das Echo von Schiffen, die länger als 30 Meter sind, ist typischerweise größer als die von den Wellen zurückgeworfene Strahlung, weshalb diese Schiffe zuverlässig erkannt werden können.

Häufig werden bei einem Angriff kleine Seefahrzeuge eingesetzt, deren Radarecho, insbesondere bei hohem Wellengang, ein Navigationsradar nicht erfassen kann.[26] Der Nutzen eines Radars ist in diesen Fällen somit als sehr gering einzuschätzen.

Kleine Schiffe ohne vorgeschriebenen Radarreflektor werden nur unzuverlässig erkannt.

Um dennoch eine Abbildung von Schiffen unter 30 Metern Länge zu ermöglichen, können die Reflektionen der Wellen anhand von bestimmten Signalverarbeitungsverfahren herausgefiltert werden.[27] Mit entsprechenden Signalverarbeitungsalgorithmen kann so die Reichweite für eine zuverlässige Detektion und Verfolgung von Objekten, wie z.B. kleinen aufblasbaren Schlauchbooten, auch bei hohem Wellengang auf bis zu 15 nautische Seemeilen ausgeweitet werden.[28] Hierdurch lässt sich der Nutzen eines Radars signifikant erhöhen.

Viele Annäherungen bei einem Angriff finden von achtern statt.[29] Ein Bereich, den Navigationsradare nur unzureichend abdecken. Diese Sicherheitslücke ließe sich ef-

[25] Wolff, „Radar Basics“.

[26] Panagopoulos und Soraghan, „Small-target detection in sea clutter“, 1355,1360.

[27] Raytheon Anschütz, „Download Brochure: Small Target Tracker“.

[28] Ebd.

[29] Witherby Seamanship International Ltd, „BMP3 Best Management Practice 3 - Piracy off the Coast of Somalia and Arabian Sea Area“, 9.

fektiv mit einem am Heck des Schiffes angebrachten Yachtradar schließen.[30] Bei der Verwendung von geeigneten Radarsystemen ergibt sich ein erheblicher Nutzen in Hinblick auf die Detektion von Angriffen. Die Radare, die zurzeit überwiegend verwendet werden, bieten hingegen nur einen geringen Nutzen. Diese Ansicht wurde in der durchgeführten Expertenbefragung ebenfalls bestätigt. Demzufolge ist der Einsatz von Radar als Detektionstechnologie nur sinnvoll, wenn einerseits ein Yachtradar am Schiffsheck verwendet wird und andererseits Schiffe, die kleiner als 30m sind, vom Radar erkannt werden können, also ein speziell für Piratenabwehr geeignetes Radarsystem verwendet wird.

MACHBARKEIT

Die Machbarkeit ist gegeben, da Radare bereits zahlreich auf Schiffen verwendet werden.

3.1.2 Nachtsichtgeräte

Zur Ergänzung zu Ferngläsern verwenden Handelsschiffe Nachtsichtgeräte, mit denen auch bei schlechten Lichtverhältnissen eine Überwachung der Umgebung des Schiffes gewährleistet werden kann.

Nachtsichtfernglässers sind eine sinnvolle Ergänzung zu Ferngläsern.

KOSTEN

Tabelle 4: Nachtsichtgeräte

Technologie	Nachtsichtgeräte
Komponenten	• Nachtsichtgerät
Bezugseinheit	• Schiff
Investitionskosten	• Hardwarekosten variieren stark • z.B. 4.480€ Zeiss Nachtsichtgerät Victory NV 5,6x62 T*[31] • z.B. 33€ Bushnell Savana[32] • z.B. 159,95€ BRESSER 5X50 DIG[33] • Softwarekosten nicht bekannt • Schulungskosten nicht bekannt
Laufende Kosten	• Nicht bekannt

NUTZEN

Nachtsichtgeräte oder Nachtsichtferngläser sind eine sinnvolle Ergänzung zu den auf Handelsschiffen verwendeten Ferngläsern. Auch wenn in der Vergangenheit ein

[30] Knott, „The Paradox of Modern-day Piracy off Somalia: The dangers, and how to reduce them“.

[31] Frankonia Handels GmbH & Co.KG, „Victory NV 5,6x62 T* von Zeiss - Nachtsichtgeräte - Optik - Frankonia.de“.

[32] Kotte & Zeller GmbH, „Savana Nachtsichtgerät güstig online bestellen im Bushnell Nachtsichtgeräte Shop - Kotte & Zeller Online Store Versand preiswert kaufen“.

[33] Reichelt Elektronik, „BRESSER 5X50 DIG Optische Geräte, Ferngläser, Microskope, Teleskop - reichelt elektronik - Der Techniksortimenter - OnlineShop für Elektronik, Netbooks, PC-Komponenten, Kabel, Bauteile, Software & Bücher - ISO 9001:2000 Zertifiziert“.

Großteil von Angriffen tagsüber stattfand, wird damit gerechnet, dass der Anteil nächtlicher Vorfälle ansteigt, womit auch der Bedarf einer Überwachung in der Nacht größer wird.[34] Hier können Nachtsichtgeräte einen wichtigen Beitrag leisten. Von den befragten Experten wurden Nachtsichtgeräte ebenfalls als empfehlenswerte Technologie eingeschätzt. Einschränkend hierzu ist jedoch zu beachten, dass das IMB empfiehlt, in durch Piraterie gefährdeten Gebieten die Oberdecksbeleuchtung einzuschalten, wodurch die Einsetzbarkeit von Nachtsichtgeräten stark eingeschränkt wird.

MACHBARKEIT

Nachtsichtgeräte existieren bereits und werden ebenfalls auf Schiffen eingesetzt. Folglich ist die Machbarkeit gegeben.

3.1.3 Kameras

Optimalerweise arbeiten die Kameras sowohl im infraroten als auch sichtbaren Lichtspektrum.

Ein System von fest installierten oder beweglichen Kameras kann bestimmte Bereiche an Bord eines Schiffes und in seiner Umgebung überwachen. Damit können ein Eindringen oder verdächtige Aktivitäten erkannt, oder wenn ein Verdachtsmoment, etwa aufgrund einer auffälligen Radarsignatur, besteht, dieses überprüft werden.[35] Im Idealfall beinhaltet das System sowohl im infraroten als auch sichtbaren Spektrum arbeitende Kameras, um zu allen Tageszeiten Bilder liefern zu können.

KOSTEN

Tabelle 5: Kameratechnologie

Technologie	Kameratechnologie
Komponenten	• Infrarotkameras oder Wärmebildkameras
Bezugseinheit	• Schiff oder Hafen
Investitionskosten	• Preisbeispiele für Infrarot- und Wärmekameras: • z.B. FLIR Navigator: 6.300€[36] • z.B. OceanView Technologies Apollo II: ca. 9.500€[37] • z.B. Fluke Ti32: ca. 8.500€[38] • Softwarekosten nicht bekannt • Schulungskosten nicht bekannt
Laufende Kosten	• Nicht bekannt

[34] Office of Naval Intelligence, „Horn of Africa: Threat Factors for Commercial Shipping and Forecast of Pirate Activity Through 2009“, 5.

[35] Urciuoli, „Supply chain security — mitigation measures and a logistics multi-layered framework“, 12-13.

[36] Seglermagazin.de, „Seglermagazin.de: Professionelle Wärmebildkameras werden bezahlbar“.

[37] NauticExpo 2010, „OceanView Technologies Launches Apollo II HD, High Definition Thermal Camera - OceanView Technologies“.

[38] Fluke, „Ti 32 Wärmebildkamera für industrielle Anwendungen, Bauthermografie, Infrarotkamera - Fluke Deutschland“.

NUTZEN

Der große Vorteil beim Einsatz von Kameras besteht darin, dass die Auswertung der Bilder auf einem Bildschirm nur einen geringen personellen Aufwand verlangt und gleichzeitig eine Abdeckung weit voneinander entfernter Bereiche ermöglicht. Sollte ein Angriff stattfinden, bei dem die Angreifer mit Waffen auf das Schiff feuern,[39] ist es für die Besatzung gefährlich zu überwachen, ob es den Angreifern gelingt, das Schiff zu entern. Die Verwendung eines Kamerasystems erlaubt es, den Vorgang des Angriffs von einem sicheren Standort zu verfolgen. Wenn Abwehrmaßnahmen ferngesteuert ausgelöst werden sollen, müssen Kamerasysteme angebracht sein.

Verfügt ein Schiff über einen Sicherheitsraum, in den sich die Besatzung im Fall eines Angriffs zurückzieht und so dem Zugriff der Angreifer entzieht, sollte dieser mit einem Bedienelement für ein vorhandenes Kamerasystem ausgestattet sein. Dies ermöglicht es der Besatzung vom Sicherheitsraum aus die Situation auf dem Schiff zu überblicken und gegebenenfalls sogar Hinweise zur Situation an Marine- oder Sicherheitskräfte weiterzugeben. Darüber hinaus wurde im Expertenworkshop empfohlen, auch für Technologien aus den Bereichen „Verzögerung“ und „Reaktion“ Kameras als Hilfsmittel einzusetzen, zum Beispiel beim Einsatz von Wasserkanonen. Besteht an Bord eines Schiffes ein Sicherheitsraum, so sollten von diesem Raum aus sowohl Bereiche um das Schiff, als auch das Schiff selber mit Kameras einsehbar sein.

MACHBARKEIT

Kameras werden bereits in vielen Bereichen und an Bord von Schiffen eingesetzt. Die Machbarkeit ist somit praktisch bewiesen.

3.1.4 Sonar

Sonar dient als „Unterwasser-Radar“ zur Erkennung von Objekten Unterwasser.

Prinzipiell funktioniert ein Sonar wie ein Unterwasserradar, wobei es anstatt von elektromagnetischen Wellen Schallwellen einsetzt. Im Wasser wird die Energie von Schallwellen nur wenig absorbiert, mit der Folge, dass Schallwellen eine weite Strecke im Wasser zurücklegen können. Die Aufgabe eines Sonars ist eine Detektion von untergetauchten oder auf der Wasseroberfläche schwimmenden Objekten und die Bestimmung der Entfernung, Bewegungsrichtung und Geschwindigkeit der Objekte.[40]
Es wird zwischen zwei verschiedenen Typen von Sonar unterschieden:[41]

- Ein aktives Sonar besteht aus einem Transmitter, der ein Signal erzeugt, und einem Empfänger, der das von einem Objekt reflektierte Echo empfängt.

- Ein passives Sonar besteht nur aus einem, oder einer Reihe von Empfängern, welche den Schall aufnehmen, den ein Objekt emittiert.

[39] Ein solches Vorgehen ist geläufig bei Piratenüberfällen vor Somalia. Das Abfeuern der Waffen soll den Kapitän einschüchtern und zu einem Verlangsamen oder Stoppen des Schiffes bewegen. Witherby Seamanship International Ltd, „BMP3 Best Management Practice 3 - Piracy off the Coast of Somalia and Arabian Sea Area“, 10.

[40] Ainslie, *Principles of Sonar Performance Modelling*, 3.

[41] Ebd, 4.

KOSTEN

Tabelle 6: Aktives Sonar

Technologie	Aktives Sonar
Komponenten	• Sonar
Bezugseinheit	• Schiff
Investitionskosten	• z.B. L3 Elac Nautic GmbH: Hardware für Subeye Multifunktionssonar kostet je nach Ausstattung ca. 750.000€ • Die Installation kostet je nach Ausführung ca. 50.000€ • Schulungskosten: ca. 15.000€[42]
Laufende Kosten	• Jährliche Wartung: ca. 5.000€[43]

NUTZEN

Ein Sonar hat verschiedene militärische, zivile, und wissenschaftliche Anwendungen. Von besonderem Interesse im Zusammenhang mit der maritimen Sicherheit sind dabei die Suche von Minen, das Aufspüren und Bekämpfen von Tauchern, die Detektion von anderen Unterwasserfahrzeugen sowie das Erkennen von Überwasserschiffen. Ein Sonar ist in der Theorie insbesondere bei einer Detektion von kleinen schnellen Booten, die nur ein geringes Radarecho erzeugen und deshalb schwer mit einem Radar erfasst werden können, vorteilhaft. In der Praxis erweist sich das Orten von Objekten an der Oberfläche mittels Sonar jedoch ebenfalls als problematisch. Zudem erfordert die zuverlässige Benutzung eines Sonars umfangreiche Erfahrung des Bedieners.

Sonare für die zivile Verwendung verbinden aktive und passive Sonare. Sie ermöglichen das Erkennen und Verfolgen von Objekten in einer Entfernung von 3.000 Metern. Neben dem aktiven Scannen der Umgebung des Schiffes erkennen sie sich schnell nähernde Boote aufgrund ihrer typischen Geräuschsignatur und können selbst Taucher unter Wasser zuverlässig identifizieren.[44] Im Expertenworkshop wurde das Sonar in Szenarien mit Piraterie-Kontext als ungeeignet bewertet, da sich dessen Detektionsmöglichkeiten auf die Überwachung unterhalb der Wasseroberfläche beziehen und im Zusammenhang mit Piraterie besonders der Bereich auf dem Wasser beobachtet werden muss. Im Zusammenhang mit Terrorismus unterschied sich die Meinung der Experten von der obigen Bewertung, da Minen- oder U-Bootangriffe mit terroristischer Motivation als realistisch eingeschätzt wurden. Gemäß den Exper-

[42] Dührkop, „Preisanfrage passives Sonar“.
[43] Ebd.
[44] L-3 ELAC Nautik, „Multipurpose Sonar SUBEYE - Safety and Security for Mega Yachts and Cruise Ships“.

ten könnte in diesem Kontext Sonartechnologie verwendet werden, um Unterwasser-Angriffe zu detektieren.

MACHBARKEIT

Die Machbarkeit wurde zwar bereits praktisch auf Schiffen bewiesen. Die befragten Experten halten eine allgemeine Ausstattung von zivilen Schiffen mit einem Sonar dennoch für unrealistisch. Zivile Schiffe sollten ohnehin Minengebiete umfahren. Im Zusammenhang mit Piraterie raten die Experten von einem Einsatz zur Detektion ab.

3.1.5 Unmanned Aerial Vehicle

Unmanned Aerial Vehicle (UAV) sind ferngesteuert oder autonom operierende Fluggeräte. Sie finden eine weite Anwendung im Rahmen von militärischen Aufklärungsoperationen.

KOSTEN

Tabelle 7: Unmanned Aerial Vehicles

Technologie	Unmanned Aerial Vehicles (UAV)
Komponenten	• UAV
Bezugseinheit	• Schiff
Investitionskosten	• Abhängig von Hersteller, Reichweite und technischen Charakteristika • Stückkosten variieren stark [45] • z.B. ca. 257.460€ ($ 350.000) (Shadow von AII) • z.B. ca. 735.601€ ($ 1 Million) (Pioneer von AII) • z.B. ca. 882.721€ ($ 1,2 Mio.) (Hunter von Northrop Grumman) • z.B. ca. 3.310.204€ ($ 4,5 Mio.) (Predator von General Atomics) • z.B. ca. 41.929.257€ ($ 57 Mio.) (Global Hawk von Northrop Grumman) • Softwarekosten nicht bekannt • Schulungskosten nicht bekannt
Laufende Kosten	• Nicht bekannt

NUTZEN

Zur Steigerung der maritimen Sicherheit können zivile UAV das Schiffsradar bei der Überwachung der Schiffsumgebung ergänzen. Außerdem könnten UAV eingesetzt werden, um potentiell feindselig gesinnte Schiffe aus großer Entfernung genauer zu betrachten. UAV bieten somit einen deutlichen Nutzen zur frühzeitigen Detektion von Angreifern.

[45] Bone und Bolkcom, „Unmanned Aerial Vehicles: Background and Issues for Congress“.

MACHBARKEIT

Begrenzt wird die Praktikabilität von UAV durch die relative geringe Reichweite ziviler Systeme, hohe Kosten für die Anschaffung, dem Bedarf von speziell geschultem Bedienpersonal und der Schwierigkeit des Landens in einem maritimen Umfeld.[46] Grundsätzlich ist die technische Machbarkeit jedoch gegeben.

UAV finden im militärischen Bereich häufiger Anwendung als im zivilen Bereich.

In den Expertenworkshops wurde die Verwendung von UAV auf Grund der hohen Kosten als unrealistisch und damit ungeeignet bewertet.

3.2 Schiffsgebundene Systeme zur automatischen Detektion eines Angriffs

Ebenso wie schiffsgebundene Systeme zur Unterstützung der Detektion eines Angriffs sollen Schiffsgebundene Systeme zur automatischen Detektion dabei helfen, im Fall eines Angriffs diesen so früh wie möglich zu erkennen. Der Unterschied der automatischen Erkennung liegt darin, dass sie darauf ausgelegt sind, verdächtiges Verhalten oder einen Angriff automatisch zu erkennen und durch das Auslösen eines Alarms anzuzeigen.

3.2.1 Softwareunterstützte Kamerasysteme

Eine entscheidende Ergänzung für sowohl im optischen als auch infraroten Bereich arbeitende Kamerasysteme kann eine entsprechende Softwareunterstützung sein. Nähert sich dem Schiff ein Objekt, wird es durch die Software automatisch erkannt und verfolgt. Bestimmte Regeln sind in der Software festgelegt, die bei einem gewissen Verhalten des verdächtigen Objektes, zum Beispiel einer Annäherung über eine festgelegte Entfernung hinaus, einen Alarm auslösen.[47]

Softwareunterstützte Kamerasysteme ermöglichen Personaleinsparungen.

KOSTEN

Die Kosten solcher Systeme hängen von den Gegebenheiten auf dem Schiff ab und können generell nicht ermittelt werden.

NUTZEN

Diese Softwareunterstützung ermöglicht eine automatische Auswertung der Bilder und kann damit den Personalaufwand reduzieren. Angriffe können zusätzlich gegebenenfalls zuverlässiger erkannt werden.

MACHBARKEIT

Diese Art von Überwachungssystemen existieren bereits in anderen Industriezweigen als der Schifffahrt. Eine Anwendung auf Schiffen ist zurzeit eher unüblich, jedoch technisch durchaus machbar. Eine vollständige automatische Überwachung ohne Personal ist aktuell noch nicht möglich. Die befragten Experten beurteilten den Einsatz dieser Technologie als sinnvoll.

[46] Knott, „The Paradox of Modern-day Piracy off Somalia: The dangers, and how to reduce them“.

[47] Urciuoli, „Supply chain security — mitigation measures and a logistics multi-layered framework“, 12-13.

3.2.2 Einbruchsdetektion

Einbruchsdetektoren erkennen einen Angriff erst beim Eindringen an Bord

Eine weitere Möglichkeit einer automatischen Detektion von Angriffen bietet sich bei dem Einsatz von Einbruchsdetektoren. Hierbei handelt es sich um Sensoren, die an kritischen Punkten an Bord platziert werden. Es eignen sich dazu etwa Bewegungsmelder, Lichtschranken, Türöffnungssensoren oder Drucksensoren.

Verfügt ein Schiff über einen Elektrozaun kann dieser auch genutzt werden, um ein unerlaubtes Betreten des Schiffes zu detektieren. Ein Elektrozaun kann jedoch auch zur Verzögerung eines Angriffs dienen. Solche Verzögerungstechnologien werden im folgenden Arbeitspapier der TUHH genauer thematisiert.

KOSTEN

Tabelle 8: Bewegungsmelder

Technologie	**Bewegungsmelder**
Komponenten	• Infrarot-Bewegungsmelder
Bezugseinheit	• Container/Schiff
Investitionskosten	• Mengenrabatte möglich • 48,96€ pro Stk. ab 1Stk. • 44,55€ pro Stk. ab 3 Stk. • 38,68€ pro Stk. ab 10 Stk.[48] • Software- und Schulungskosten nicht bekannt
Laufende Kosten	• Nicht bekannt

[48] Conrad Electronic SE, „Bewegungsmelder 10 A, Serie 18“.

Tabelle 9: Lichtschranke

Technologie	Lichtschranke
Komponenten	• Lichtschranke
Bezugseinheit	• Container/Schiff
Investitionskosten	• Auflistung der Kosten für einige Beispielgeräte (Preise variieren je nach Ausführung): • z.B. IRS 100: IR-Reflexions-Lichtschranke: 79,95€[49] • z.B. Contrinex LLK-5050-003 Einweg-Lichtschranke: 33,39€[50] • z.B. ABUS Lichtschranke LS 1020: 47,95€ • z.B. ABUS Lichtschranke LS 2030: 96,95€ • z.B. ABUS Lichtschranke LS 2060: 135,00€[51]
Laufende Kosten	• Nicht bekannt

Tabelle 10: Drucksensor

Technologie	Drucksensor
Komponenten	• Drucksensor
Bezugseinheit	• Container/Schiff
Investitionskosten	• Auflistung der Kosten für einige Beispielgeräte (Preise variieren je nach Ausführung): • z.B. Drucksensormodul mit Spannungsausgang/I2C Hygrosens DRMOD-I2C-R6B 0 - 6 bar 6 - 15 V: 83,00€ • z.B. Drucksensor 26PC-Serie Honeywell 26PCBFM6G: 30,56€ • z.B. Analoger Differenzdrucksensor SDP-Serie Sensirion SDP1000-L 0 - 500 Pa 5 V/DC: 109,35€[52]
Laufende Kosten	• Nicht bekannt

[49] Reichelt Elektronik, „IRS 100 Alarmsensoren & Zubehör - reichelt elektronik - Der Techniksortimenter - OnlineShop für Elektronik, Netbooks, PC-Komponenten, Kabel, Bauteile, Software & Bücher - ISO 9001:2000 Zertifiziert“.

[50] Conrad Electronic SE, „Quadratische Lichtschranke Contrinex LLK-5050-003 Einweg-Lichtschranke (Empfänger) Reichweite 15000 mm im Conrad Online Shop“.

[51] ELV Elektronik AG, „ABUS Lichtschranke LS 1020 | ELV-Elektronik“.

[52] Conrad Electronic SE, „Druck-Sensoren-Sortiment im Conrad Online Shop“.

NUTZEN

Einbruchsdetektoren ermöglichen erst eine Erkennung eines Angriffs an Bord des Schiffes. Ein frühzeitigeres Erkennen von Angreifern ist nicht möglich. Somit können auch keine frühzeitigen Maßnahmen zur Abwehr des Angriffs eingeleitet werden. Einbruchsdetektoren können lediglich dazu verhelfen, im letzten Moment Gegenmaßnahmen zu ergreifen.

MACHBARKEIT

Einbruchsdetektoren stellen keine hohen Voraussetzungen an die Technik. Sie werden bereits in vielen Bereichen verwendet. Die im Workshop befragten Experten bewerteten den Einsatz dieser Technologie als wenig sinnvoll, da die Piraten sich bereits in unmittelbarer Nähe oder direkt auf dem Schiff befinden, wenn die Detektoren den Angriff erkennen. Bei einer so geringen Entfernung ist die Wahrscheinlichkeit sehr hoch, dass die Piraten bereits mit einer anderen Technologie detektiert wurden, oder schon mit bloßem Auge erkannt werden können. Im Regelfall bleibt nach der Einbruchsdetektion nicht ausreichend Zeit, um geeignete Gegenmaßen zu ergreifen.

3.2.3 Ship Infrared Monitoring, Observation and Navigation Equipment

SIMONE ermöglicht mithilfe von Infrarotsensoren eine lückenlose Überwachung des Schiffsumfeldes.

Ein Beispiel für ein bis zur Marktreife entwickeltes System, das mithilfe von Infrarotsensoren eine lückenlose Überwachung des Schiffsumfeldes im Nah- und Nächstbereich ermöglicht, ist das Ship Infrared Monitoring, Observation and Navigation Equipment (SIMONE) der Firma Diehl.

Das System besteht aus mehreren Infrarot-Sensormodulen, welche in die Bordwand des Schiffes integriert werden. Optional sind darüber hinaus Kameras Teil des Systems.

KOSTEN

Detaillierte Kosten für die Implementierung dieses Systems konnten nicht ermittelt werden. Ein Auftrag zur Ausrüstung von vier Fregatten mit SIMONE über ein Volumen von mehr als sieben Millionen Euro wurde bereits im März 2009 erteilt.[53]

NUTZEN

Durch die Infrarot-Sensoren lassen sich Personen, Schwimmer, Schlauchboote und Schiffe auf See und sogar Bedrohungen aus der Luft, zum Beispiel durch Drohnen oder Flugzeuge, zuverlässig erkennen[54]. Schlechte Wetterbedingungen, insbesondere Regen, Nebel etc., beeinträchtigen die Reichweite und Zuverlässigkeit der Infrarot-Sensoren.

Die erfassten Objekte werden detektiert, verfolgt und in Gefahrenstufen eingeordnet, für welche sich wiederum automatisierte Alarmkreise definieren lassen. In ei-

[53] Europäische Sicherheit, „Diehl Defence auf Wachstumskurs“.

[54] Diehl BGT Defence, „Diehl BGT Defence | Sensoren“.

nem zentralen Leitstand werden die Informationen zusammengeführt und dargestellt.

MACHBARKEIT

Obwohl die technische Machbarkeit gegeben ist, ist angesichts dieser hohen Kosten ein Einsatz von entsprechenden Systemen in der zivilen Schifffahrt unwahrscheinlich und für die nahe Zukunft nicht zu erwarten. Die im Workshop befragten Experten argumentierten gegen den Einsatz von Infrarot-Systemen. Sie bewerteten den Mitteleinsatz (Kosten) als unangemessen hoch.

3.2.4 Pirate and Terrorist Aversion System

PITAS verbindet eine Vielzahl an Sensoren miteinander und analysiert die Daten in Echtzeit.

Pirate and Terrorist Aversion System (PITAS) ist ein Forschungsvorhaben, in dem verschiedene Partner aus Wirtschaft und Wissenschaft Schleswig-Holsteins und Hamburgs zusammenarbeiten, u.a. ThyssenKrupp Marine Systems, Hamburg, Raytheon Anschütz GmbH, Kiel, Fachhochschule Kiel sowie die Technische Fakultät der Christian-Albrechts-Universität zu Kiel. Das PITAS sieht vor, verschiedene Sensoren eines Schiffes, etwa Radar, Sonar und Kameras, in einem System einzubinden. Die gewonnenen Daten aus den verschiedenen Quellen werden in Echtzeit verarbeitet und analysiert. Ergebnis der Verarbeitung ist ein Erkennen von Objekten in der Umgebung des Schiffes und eine elektronische Darstellung der Objekte in Verbindung mit dem aktuellen Kartenmaterial. Das Verhaltensmuster dieser Objekte wird in einem ersten Schritt analysiert und durch Informationen aus einer Datenbank (z.B. Schiffsidentifikationsdateien, -profil, Signaturen bekannter Objekte u. ä.) ergänzt. In einem zweiten Schritt der Analyse wird das Verhalten eines identifizierten Objektes mit bekannten Verhaltensmustern verglichen, von denen in der Vergangenheit keine Gefahr ausging beziehungsweise für welche bekannt ist, dass sie im Zusammenhang mit einem Angriff vorkommen.

KOSTEN

Die Kosten für dieses System konnten nicht ermittelt werden. Eine Datenverarbeitung und –analyse in Echtzeit führen jedoch zu hohen Kosten.

NUTZEN

Tritt eine Abweichung von bekannten Verhaltensmustern auf oder werden gefährliche Verhaltensmuster identifiziert, wird von dem System automatisch ein Alarm ausgelöst, um die Besatzung auf die mögliche Gefahr aufmerksam zu machen. Vorgesehen ist darüber hinaus, dass das System im Fall einer erkannten Bedrohung automatisch die Einleitung von Reaktionsmaßnahmen übernimmt.

MACHBARKEIT

Die Technologie befindet sich noch im Entwicklungsstadium und ist daher noch nicht einsetzbar. Eine grundsätzliche Machbarkeit scheint jedoch gegeben zu sein. Auf Grund des frühen Entwicklungsstadiums konnte im Expertenworkshop keine Beur-

teilung zum Einsatz dieser Technologie getroffen werden. Es wurden jedoch Bedenken aufgrund hoher angenommener Kosten geäußert.

3.3 Bereichsüberwachung zur Erfassung potentieller Angreifer

Die Überwachung eines Seegebietes ermöglicht es, eine Gefahrenquelle bereits zu identifizieren, bevor es zu einem Angriff kommt.

Die bei der Bereichsüberwachung eingesetzten Technologien unterscheiden sich im Hinblick auf den Ort der Installation. Möglich ist eine Überwachung von Land, Luft, Wasser und dem Weltraum aus.

3.3.1 Unmanned Underwater Vehicle

Ein Unmanned Underwater Vehicle (UUV) ist ein selbstfahrendes, vollkommen autonomes (entweder nach vorbestimmten oder in Echtzeit angepassten Missionszielen) oder mit minimaler Steuerung unter der Wasseroberfläche operierendes Fahrzeug.[55]

UUV können Gefahren Unterwasser unabhängig von betroffenen Schiffen detektieren.

Um die Sicherheit der zivilen Schifffahrt zu gewährleisten, können UUV zur Minensuche eingesetzt werden. Dabei werden Schifffahrtswege auf zum Zweck eines Angriffs platzierte Minen überprüft, um so eine ungefährdete Passage zu ermöglichen.

KOSTEN

Tabelle 11: Unmanned Underwater Vehicles (UUV)

Technologie	Unmanned Underwater Vehicles (UUV)
Komponenten	• UUV
Bezugseinheit	• Schiff
Investitionskosten	• Kleines UUV: 36.780€ - 183.900€ • Mittleres UUV: 183.900€ - 735.601€ • Großes UUV: 735.601€ - 3.678.005€[56] • Softwarekosten nicht bekannt • Schulungskosten für Programmierung des UUVs nicht bekannt
Laufende Kosten	• Nicht bekannt

NUTZEN

UUV stellen kein umfassendes System zur Detektion dar. Sie können jedoch Gefahren Unterwasser effektiv erkennen. Gegen andere Gefahren bieten sie keinen Schutz. Die Gefahren, die UUV erkennen können, betreffen insbesondere den Bereich des maritimen Terrorismus. Der Schutz gegen Piraterie ist als gering zu bewerten.

[55] US Navy, „The Navy Unmanned Undersea Vehicle (UUV) Master Plan“, 4. Ebd, 5.Ebd, 5.Ebd, 5.Ebd, 5.

[56] NewmanPaul, „Unmanned vehicles for schallow and coastal waters“.

MACHBARKEIT

Die zur Entwicklung von UUV benötigte Technologie ist ausgereift und verfügbar. Mögliche, für die nahe Zukunft anvisierte Anwendungen von UUV sind Minensuche, U-Boot Bekämpfung, Ozeanographie und die Aufklärung von Umweltbedingungen.[57] Die befragten Experten bewerteten den Bereich „Unterwasser" jedoch als irrelevant für die Detektion von potentiellen Angriffen durch Piraten. Hintergrund für diese Bewertung ist die Tatsache, dass bei den meisten Piraterie-Angriffen der Vergangenheit nur Überwasser-Angriffsboote genutzt wurden. Für die Detektion von terroristischen Bedrohungen wurde die Verwendung der Technologie zwar als zweckdienlich bewertet, jedoch auf Grund der Investitionskosten als unrealistisch eingestuft.

3.3.2 Satellitenüberwachung

Satelliten ermöglichen eine großflächige Überwachung von Seegebieten als Ergänzung zu weiteren Detektionstechnologien.

Satellitenbasierte Überwachungssysteme können einen Beitrag zur Kontrolle von Seegebieten leisten und die Reichweite der maritimen Aufklärung vergrößern. Sie erfüllen dabei die Funktionen des regelmäßigen Beobachtens eines großen Bereiches und der Identifikation möglicher Gefahren und auffälligem Verhalten. Damit ergänzen sie andere land-, wasser- und luftbasierte Systeme wie etwa Radar AIS oder Luftüberwachung und zeichnen sich insbesondere durch ihre globale Einsetzbarkeit aus. Sie sind zum Beispiel gut geeignet, um lange Küstenabschnitte zu untersuchen, die einen möglichen Ausgangspunkt für Angriffe auf See darstellen könnten.[58]

Im Rahmen der Überwachung mit Hilfe von Satelliten werden optische Geräte, die das gesamte Spektrum von sichtbarem bis infrarotem Licht abdecken, eingesetzt. Diese sind jedoch an wolkenlose Bedingungen gebunden. Ebenso finden Radarsysteme, insbesondere Synthetic Aperture Radar (SAR), Verwendung, welche auch bei wolkenverhangenem Himmel funktionieren, jedoch nur eine ungenauere Auflösung ermöglichen.[59]

KOSTEN

Tabelle 12: Satellitenüberwachung

Technologie	Satellitenüberwachung
Komponenten	• Festeingebautes oder autarkes Containerortungsmodul • Satellit zur Ortung • Software, um Containerposition anzugeben
Bezugseinheit	• Container
Investitionskosten	• Containerortungsmodul • Software im Internet zugänglich
Laufende Kosten	• Nicht bekannt

[57] National Research Council, *Autonomous Vehicles in Support of Naval Operations*, 124.

[58] Remuss, „Space Applications as a Supporting Tool for Countering Piracy – Outline for a European Approach", 21, 32.

[59] Ebd, 34.

Die Kosten für die in der obigen Tabelle genannten Komponenten können nicht ermittelt werden, da die Anbieter keine Preise veröffentlichen.

NUTZEN

Die Untergrenze einer Erfassung von Schiffen liegt aktuell für optische Systeme bei 8-10 Metern und für SAR-Systeme bei etwa 30 Metern Länge des Schiffes. Radar-Systeme sind daher besonders geeignet, Schiffe zu entdecken; optische Systeme, um eine Klassifizierung der Schiffe vorzunehmen.[60]

Ein Erfassen und Verfolgen von mittleren bis großen Schiffen ist mit satellitenbasierten Überwachungssystemen gut möglich, für kleine Boote jedoch nicht. Um festzustellen, ob von identifizierten Schiffsbewegungen eine potentielle Gefahr ausgeht, bedarf es einer Auswertung der Bilder und zusätzlicher nachrichtendienstlicher Informationen.[61]

Zur Untersuchung von langen Küstenabschnitten, die einen möglichen Ausgangspunkt für Angriffe auf See darstellen könnten, kann die Satellitenüberwachung effektiv eingesetzt werden.[62]

MACHBARKEIT

Satellitenüberwachung existiert bereits und ist somit technisch machbar. Auf Grund der beobachteten Häufung der Piratenangriffe durch kleine Boote, bewerteten die Experten den Einsatz von Satellitenüberwachung als wenig sinnvoll.

3.3.3 Vessel Ortung und Tracking

VTS ermöglichen es, die Route eines Schiffes zu verfolgen.

Vessel Tracking Systeme (VTS) ermöglichen es, die Position eines Schiffes zu verschiedenen Zeitpunkten zu bestimmen und somit seine Route zu verfolgen. So ist für den Fall, dass ein Angriff auf ein Schiff stattfindet, und es gelingt, diesen an eine Sicherheitsinstanz zu melden, die genaue Position des Schiffes bekannt. Dies ist die Voraussetzung, um in der Nähe befindliche Sicherheitskräfte so schnell wie möglich an den Ort des Vorfalls zu bringen. Weiter ist es bei der Existenz eines VTS möglich, sollten Angreifer erfolgreich die Kontrolle über ein Schiff übernehmen, die Bewegung des Schiffes zu verfolgen, um daraus Rückschlüsse auf die Absichten der Angreifer zu ziehen.

Generell sind verschiedene Konzepte denkbar, mit denen ein Schiff geortet werden kann. Die Positionsbestimmung an Bord erfolgt mit einem GNSS. Für die Übermittlung der Daten bieten sich eine Übertragung mit elektromagnetischen Wellen auf direktem Weg, zum Beispiel mit Ultrakurzwellen, oder mit dem Umweg über einen Satelliten an. Ein Beispiel für ein kommerzielles System, welches Schiffseignern eine Ortung und Verfolgung ihrer Schiffe erlaubt, ist ShipLoc.[63] Die Verwendung eines entsprechenden Systems wird vom International Maritime Bureau empfohlen.[64]

---

[60] Ebd, 80.
[61] Ebd, 48-49.
[62] Ebd, 21, 32.
[63] Kathert, *Piraterie auf See*, 84.

KOSTEN

Die Kosten für Vessel Tracking Systeme konnten nicht ermittelt werden.

NUTZEN

VTS können grundsätzlich nicht zur Entdeckung von Angriffen beitragen. Sie können lediglich den Ort bestimmen. Vorsetzung ist jedoch immer eine Detektion eines Angriffs. VTS stellen eine sinnvolle Ergänzung zu weiteren Detektion-Technologien dar.

MACHBARKEIT

VTS werden bereits verwendet und stellen keine besonderen Anforderungen an die Technik. Die Machbarkeit ist somit gegeben und der Einsatz der Technologie wurde als Ergänzung zu den direkten Detektionstechnologien von den Experten empfohlen.

Ein entsprechendes System zur Positionsbestimmung eines Schiffes könnte auch analog, wie für Container im Rahmen eines Geofencing[65], verwandt werden, um automatisch die Route des Schiffes zu überwachen und bei einem Abweichen einen Alarm auszulösen.

3.3.4 Automatisches Schiffs-Identifizierungssystem

AIS dient der Schiffsidentifizierung und gehört weitgehend zur Standardausrüstung.

AIS steht für Automatisches Schiffs-Identifizierungssystem (Automatic Identification System). Mit AIS identifizieren sich Schiffe und geben relevante statische, reisebezogene und dynamische Daten für andere eindeutig bekannt."[66] Die Ausrüstung von Schiffen mit einer Bruttoraumzahl größer 300 auf internationaler Fahrt[67] mit AIS ist unter Kapitel 5 des SOLAS Abkommens vorgeschrieben.[68]

Die statischen mit AIS übertragenen Daten geben Auskunft über den Schiffsnamen, das Internationale Funkrufzeichen, den Schiffstyp und die Abmessungen des Schiffes. Reisebezogene Daten sind der aktuelle Tiefgang, der Bestimmungshafen, das ETA (geplante Ankunftszeit) sowie unter Umständen eine Angabe zur Ladungskategorie. Zu den für die Kollisionsverhütung mit anderen Schiffen bedeutenden dynamischen Daten zählen genaue Angaben über die Position des Schiffes, seine Geschwindigkeit und seinen Kurs über Grund, die exakte Vorausrichtung oder auch das momentane Drehverhalten des Schiffes.[69]

---

shiploc.com, „ShipLoc - About ShipLoc".

[64] Rosenberg, „The Political Economy of Piracy in the South China Sea", 87.

[65] Geofencing ist ein Kunstwort, das sich aus den englischen Begriffen „geographic" and „fence" zusammensetzt. Hierbei wird beispielsweise überprüft, ob sich ein Objekt innerhalb geographischer Grenzen (Zäunen) befindet.

[66] Bundesministerium für Verkehr-, Bau- und Wohnungswesen, „Automatic Identification System — ein neuer internationaler Standard fürdie Identifikation von Schiffen auf See", 3.

[67] Für Schiffe auf nationaler Fahrt ist ein AIS ab einer Bruttoraumzahl von 500 vorgeschrieben. Passagierschiffe müssen unabhängig von der Bruttoraumzahl mit einem AIS ausgerüstet sein.

[68] International Maritime Organization., *SOLAS*, 256.

[69] Bundesministerium für VerkehrBau- und Wohnungswesen, „Automatic Identification System — ein neuer internationaler Standard fürdie Identifikation von Schiffen auf See", 3.

Eine Datenübertragung zwischen Schiffen oder zwischen Empfängern an Land findet bei AIS auf speziellen Ultrakurzwellenfrequenzen statt. Die Reichweite einer Schiff-zu-Schiff Übertragung von AIS beträgt etwa 20 nautische Meilen. Für Empfänger an Land ist sie größer.[70]

KOSTEN

Tabelle 13: Automatisches Schiffs-Identifizierungs-System (AIS)

Technologie	Automatisches Schiffs-Identifizierungs-System (AIS)
Komponenten	• AIS Technik an Bord des Schiffes: • UKW-Sende- und Empfangseinheit • Sensoriksysteme • GNSS-Empfänger • Geräte zur Auswertung der empfangenen Daten • Internetdienste, die die Daten des Schiffes aufarbeiten
Bezugseinheit	• Schiff
Investitionskosten	• AIS-Empfänger ca. 250 – 650€ • AIS-Antenne ca. 60 – 120€ • AIS-Splitter ca. 200€[71] • Kabel zur Verbindung der Komponenten: 6 € pro 1m bzw. 40€ für 5 m[72] • AIS-Transponder Klasse B (für kleine Boote): 600 € - 1200€ • AIS –Transponder Klasse A (für AIS-pflichtige Schiffe): Bsp.: COMAR CSA200: 2280,00€[73] • Multifunktionsdisplays: 2449,00€ bis 4439,00€ (je nach Ausführung)[74] • Softwarekosten/Kosten für Internetdienste nicht bekannt • Schulungskosten nicht bekannt
Laufende Kosten	• Nicht bekannt

[70] Hoye u. a., „Space-based AIS for global maritime traffic monitoring“, 1.

[71] Busse Yachtshop, „Busse-Yachtshop - Bootszubehoer - Seekarten, Fischfinder, AIS, Radar, Wassermacher“.

[72] Y-tronic Yacht-Electronic GbR, „Y-tronic Online Shop“.

[73] SPI GmbH, „SPI Marineshop“.

[74] Busse Yachtshop, „Raymarine C90W / C120W / C140W ‚Widescreen‘ bei Busse Yachtshop“.

NUTZEN

Problematisch ist, dass die Ausrüstungspflicht mit AIS nur für verhältnismäßig große Schiffe gilt, eine Bedrohung jedoch in vielen Fällen von kleinen Booten ausgeht, die mit AIS nicht identifiziert werden können. Durch den Abgleich von AIS-Daten mit Radarinformationen können Fahrzeuge ohne AIS-Bordgerät von den übrigen Schiffen rechtzeitig unterschieden werden. Werden signaturlose Schiffe in einem Gebiet erhöhten Risikos erkannt, sollte dies der Anlass zu gesteigerter Wachsamkeit sein, da es sich um einen potentiellen Angreifer handeln könnte.

AIS Daten können von jedem empfangen werden, der ein entsprechendes Empfangsgerät besitzt. So könnten sie auch von einem Angreifer eingesetzt werden, um mögliche Ziele zu identifizieren und abzufangen. Darüber, ob ein Einsatz von AIS Daten bei Angriffen auf Schiffe im Golf von Aden unterstützend zum Einsatz kommt, gibt es divergierende Ansichten.[75] Der Gesamtnutzen ist somit nicht eindeutig zu ermitteln.

Um einen Missbrauch von AIS zu verhindern, ist ein Abstellen des Systems durch den Kapitän des Schiffes in Gebieten mit einem hohen Angriffsrisiko möglich. Wenn ein Angriff erkannt wird, sollte es jedoch unverzüglich eingeschaltet werden, um herbeigerufenen Sicherheitskräften die Bestimmung der aktuellen Position des Schiffes zu ermöglichen.[76]

MACHBARKEIT

Da ein AIS für bestimmt Schiffe vorgeschrieben ist, wurde die Machbarkeit bereits empirisch bewiesen. Die befragten Experten konnten sich auf Grund zu stark divergierender Meinungen nicht zu einer einhelligen Empfehlung kommen.

3.3.5 Long Range Identification and Tracking

LRIT ist ein satellitenunterstütztes System mit geschützten Daten.

Seit 2006 ist neben AIS mit dem Long Range Identification and Tracking (LRIT) ein weiteres System zur Identifizierung von Schiffen im Kapitel 5 des SOLAS Abkommens vorgeschrieben.[77] Im Gegensatz zu AIS ermöglicht LRIT auf Grund einer satellitengestützten Kommunikation eine globale Positionsbestimmung. Außerdem sind die LRIT Daten nicht frei empfangbar, sondern nur unter bestimmten Voraussetzungen zugänglich.

Mindestens vier Mal pro Tag werden die Identität und Position des Schiffes sowie der Zeitpunkt der Übertragung vom LRIT Gerät an Bord eines Schiffes an einen Satelliten übermittelt. Der Umfang der übermittelten Daten ist damit geringer als bei AIS. Eine Ausrüstungspflicht besteht für Frachtschiffe auf internationaler Fahrt ab einer Bruttoraumzahl von 300.[78] Die von LRIT erfassten Daten werden in einer Datenbank gespeichert und können unter bestimmten Voraussetzungen von den Vertragsregie-

[75] Office of Naval Intelligence, „Horn of Africa: Threat Factors for Commercial Shipping and Forecast of Pirate Activity Through 2009“, 1. Donner und Kruk, „Supply Chain Security Guide“, 36.

[76] Witherby Seamanship International Ltd, „BMP3 Best Management Practice 3 - Piracy off the Coast of Somalia and Arabian Sea Area“, 15-16.

[77] International Maritime Organization., *SOLAS*, 257-260.

[78] Offshore-Bohreinheiten sowie Passagierschiffe, unabhängig von ihrer Bruttoraumzahl, müssen ebenfalls ausgerüstet sein.

rungen des SOLAS sowie Seenotrettungsdiensten abgerufen werden. Unter anderem sind Vertragsregierungen berechtigt, Daten zu allen Schiffen in einer maximalen Entfernung von 1.000 nautischen Meilen von der Küste abzurufen. Die Regelung sieht vor, dass LRIT abschaltbar ist. Damit kann das System theoretisch auch von einem Angreifer abgeschaltet werden und somit seine Verwendbarkeit verlieren.[79]

KOSTEN

Tabelle 14: Long Range Identification and Tracking (LRIT)

Technologie	Long Range Identification and Tracking (LRIT)
Komponenten	• LRIT-fähige Einheit
Bezugseinheit	• Schiff
Investitionskosten	• Die meisten Schiffe sind bereits LRIT fähig → keine Investitionskosten • Neue LRIT-fähige Einheit kostet ca. 2.795€[80]
Laufende Kosten	• Es würden Kosten pro Übertragung anfallen → Kosten nicht bekannt

NUTZEN

Grundsätzlich stellt LRIT ein geeignetes System zur zuverlässigen Erkennung und Identifizierung von Schiffen dar. Allerdings ist, genau wie bei AIS, bei LRIT eine Detektion kleiner Schiffe, für die keine Ausrüstungspflicht besteht, nicht möglich. Darüber hinaus gibt es Bedenken, ob die Verbreitung von LRIT Daten in die Hände von böswilligen Parteien, welche sie nutzen um Schiffe zu identifizieren, verhindert werden kann.[81]

MACHBARKEIT

LRIT findet bereits auf Schiffen Anwendung, wodurch die Machbarkeit belegt wird. Wie bei AIS, konnten sich die befragten Experten auf Grund zu stark divergierender Meinungen nicht zu einer eindeutigen Empfehlung entschließen.

3.3.6 AISat

Bei AISat werden Daten von Satelliten empfangen und an die Erde weitergeleitet, um eine flächendeckende Überwachung zu gewährleisten.

Eine weitere Möglichkeit zur weltweiten Verfolgung und Identifikation von Schiffen ist AISat. Hierbei werden die AIS Daten von Satelliten in einer Höhe von 1.000 km empfangen und anschließend an die Erde weitergeleitet. So ist es prinzipiell möglich, die Bewegung von Schiffen, die mit einem AIS Sender ausgestattet sind, auch außerhalb der Reichweite landgestützter Empfänger zu überwachen.

Bei der praktischen Anwendung ist jedoch problematisch, dass AIS-Systeme nur eine begrenzte Anzahl von Schiffen in einem Gebiet unterstützen. Ein AIS Empfänger, der

[79] International Maritime Organization., *SOLAS*, 257-260.

[80] Canada Gazette und Val, „Canada Gazette – Long-Range Identification and Tracking of Vessels Regulations“.

[81] Donner und Kruk, „Supply Chain Security Guide“, 35.

in einem Satelliten integriert ist, deckt jedoch einen so großen Bereich ab, dass es vorkommen kann, dass sich mehr Schiffe in diesem Bereich aufhalten als erfasst werden können. Als Folge entstehen Interferenzprobleme, die zu einer Nichtabbildung führen.[82]

KOSTEN

Kosten für AISat können noch nicht bestimmt werden, da sich die AISat Technologie noch in der Entwicklungsphase befindet. Es ist anzunehmen, dass AISat mehr Kosten als das normale AIS verursachen wird.

NUTZEN

Der Nutzen eines zuverlässigen Systems zur Identifizierung wäre erheblich. Eine automatische Identifizierung könnte somit gewährleistet werden. Da die aktuelle Version keine zuverlässige Identifizierung gewährleisten kann, ist ihr Nutzen als deutlich geringer einzuschätzen.

MACHBARKEIT

In Europäischen Gewässern können nach Berechnungen von Hoye[83] bis zu 6.200 Schiffe im Bereich eines Satelliten liegen. Wenn nur diejenigen Schiffe satellitengestützt erfasst werden sollen, die außerhalb der Reichweite einer landbasierten Empfangsstation liegen, reduziert sich die Zahl auf bis zu 2.600. Ein AISat-System könnte diese Anzahl an Schiffen nicht erfassen. Eine Modifikation des Sendeintervalls und der Datenmenge könnte jedoch eine Detektion ermöglichen.[84]

3.3.7 Predictive Analysis for Naval Deployment Activities

PANDA analysiert Verhaltensmuster auf See, um Bedrohungen zu identifizieren.

Predictive Analysis for Naval Deployment Activities (PANDA) hat dasselbe Ziel wie PITAS: das Aufzeichnen von Verhaltensmustern verschiedener Objekte auf See. Aus den aufgezeichneten Verhaltensmustern kann ein „normales“ Verhalten abgeleitet werden. Wird ein von diesem normalen Verhalten abweichendes Objekt identifiziert, löst das System einen Alarm aus. Der Unterschied besteht darin, dass nicht schiffsgebundene Sensoren die Daten für die Untersuchung bereitstellen, sondern sie Vessel Ortungs- und Trackingsystemen entnommen werden.

KOSTEN

Das PANDA-System wird von einer Behörde des US-Verteidigungsministeriums entwickelt und wird mit ca. 1,5 Mio. US$ gefördert.[85] PANDA befindet sich noch in der Entwicklung, daher können keine Angaben zu eventuellen Kosten für die Nutzung getätigt werden.

[82] Hoye u. a., „Space-based AIS for global maritime traffic monitoring“, 2.
[83] Ebd, 3.
[84] Ebd, 4.
[85] Federal Business Opportunities, „Predictive Analysis For Naval Deployment Activities (PANDA)“.

NUTZEN

Durch die Verwendung von Daten aus Vessel Ortungs- und Trackingsystemen ist PANDA begrenzt auf Schiffe, die mit einem Ortungssystem ausgestattet sind. Kleine Schiffe, von denen in verschiedenen Szenarien eine Gefahr ausgeht, werden somit nicht durch das System abgebildet. Der Gesamtnutzen ist somit als gering einzuschätzen. Jedoch kann ein solches System zur Ortung von entführten Schiffen eingesetzt werden, wenn es von den Piraten bzw. Terroristen nicht entfernt wurde.

MACHBARKEIT

Da sich PANDA noch im Entwicklungsstatus befindet, ist eine Machbarkeit aktuell nicht gegeben. Die Experten äußerten sich zudem skeptisch gegenüber der Realisierbarkeit der Technologie.

4 Fazit und Ausblick

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 Bereiche kategorisiert: Detektion, Verzögerung und Reaktion. Das vorliegende Arbeitspapier fokussiert die Kategorie Detektion. Die unterschiedlichen Sicherheitstechnologien wurden zunächst auf ihre Kosten, ihren Nutzen und ihre Machbarkeit hin analysiert. In einer anschließenden Expertenbefragung wurde mithilfe von Gruppendiskussionen und Szenariotechnik die Praxistauglichkeit der identifizierten Technologien zur Bekämpfung von Piraterie und maritimen Terrorismus überprüft. In einer aggregierten Betrachtung stellten die Experten fest, dass die folgenden Technologien prinzipiell geeignet sind: Nachtsichtgeräte, Kameras, softwareunterstützte Kamerasysteme und Vessel Ortung und Tracking. Bedingt geeignet sind Radar, Einbruchsdetektoren, SIMONE, PITAS, Satellitenüberwachung, AIS, LRIT, AISat und PANDA. Als ungeeignet eingeschätzt wurden Sonar, UAV und UUV auf Grund von unverhältnismäßig hohen Kosten. In den meisten Fällen herrschte in den vier Gruppen Übereinstimmung über die Eignung der jeweiligen Technologien. Die unterschiedlichen Ausgangslagen führten jedoch für einige Technologien zu abweichenden Bewertungen. Solange eine Technologie in einem Szenario als sinnvoll bewertet wurde und in den anderen Szenarien keinen negativen zugewiesen Nutzen bekam, wurde diese Technologie insgesamt als prinzipiell geeignet erachtet.

Im Workshop wurde darüber hinaus festgestellt, dass die Bedrohung durch maritimen Terrorismus schwieriger zu bewerten bzw. das Risiko nur äußerst unpräzise einzuschätzen ist. Während es jedes Jahr eine Vielzahl von Piratenangriffen gibt, stellen maritime Angriffe durch Terroristen die Ausnahme dar. Dies führt dazu, dass für Piraterie die Gefährdungslagen in unterschiedlichen Regionen relativ verlässlich eingeschätzt werden können. Für den Bereich des maritimen Terrorismus ist dies jedoch nicht möglich. Zum einen ist das auf eine fehlende, solide Datenbasis zurückzuführen zum anderen auf eine hohe Vielfalt möglicher Anschlagsszenarien. Terroristen beabsichtigen i.d.R. einen großen Schaden bzw. eine große Aufmerksamkeit zu erzeugen und sind örtlich ungebundener. Die Vorgehensweisen von Terroristen beschränken sich nicht auf einige wenige, wie dies für somalische Piraten der Fall ist. Gewisse politische Motive erfordern unter Umständen jedoch auch hier einen Anschlag in bestimmten Regionen. So dient die Androhung des Versenkens eines gekaperten Öltankers vor der Küste der USA insbesondere als Druckmittel gegen die USA. Eine allgemeine, unpräzise und allgegenwärtige Bedrohungslage durch Terroristen erschwert die Analyse über den Einsatz von Technologien zur Bekämpfung von maritimem Terrorismus. Die Bedrohung durch Piraterie ist vergleichsweise prägnant, was die Untersuchung des Physical Protection Systems erleichtert.

Für das gesamte Physical Protection System wurden, auf das Schiff bezogen, mehr als 40 Technologien identifiziert. Davon entfallen auf die Detektionsphase 16 Stück. Für die von den Experten als geeignet eingestuften Technologien müssen Weiterentwicklungen und neue Einsatzmöglichkeiten im Detail evaluiert werden.

Die benötigten organisatorischen, strukturellen, personellen und informationstechnologischen Voraussetzungen müssen ebenfalls noch im Detail erläutert werden.

Weiterer Forschungsbedarf besteht in der Bildung geeigneter Indikatoren zur Bewertung der Vulnerabilität der Objekte Schiff und Container 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 sie nicht ausschließlich losgelöst von einander betrachtet werden. Hierfür sollte somit eine geeignete zusammenfassende Betrachtung bzw. Bewertung entwickelt werden. Eine detaillierte Analyse wird ein differenziertes Darlegen von Vulnerabilitäten und somit auch das Identifizieren von geeigneten technologischen Gegenmaßnahmen ermöglichen.

Literaturverzeichnis

Ainslie, Michael. *Principles of Sonar Performance Modelling*. Berlin, Heidelberg: Springer, 2010. http://www.springerlink.com/content/978-3-540-87661-8/contents/.

Amato, Felicia, Michele Fiorini, Sergio Gallone, und Giovanni Golino. „Fully solid state radar for vessel traffic services“. 1-5, 2010.

Blumberg, B., R. Cooper, und P. Schindler. *Business Research Methods*. McGraw-Hill Education, 2008.

Bone, Elizabeth, und Christopher Bolkcom. „Unmanned Aerial Vehicles: Background and Issues for Congress“, April 25, 2003. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA467807&Location=U2&doc=GetTRDoc.pdf.

Bundesministerium für Bevölkerungsschutz und Katastrophenhilfe, Hrsg. „Methode für Risikoanalyse im Bevölkerungsschutz“, 2010.

Bundesministerium für VerkehrBau- und Wohnungswesen. „Automatic Identification System —ein neuer internationaler Standard fürdie Identifikation von Schiffen auf See“, 2005. http://www.wsd-nordwest.de/verkehrstechnik/pdf/AIS-_Broschuere-deutsch.pdf.

Busse Yachtshop. „Busse-Yachtshop - Bootszubehoer - Seekarten, Fischfinder, AIS, Radar, Wassermacher“, Dezember 20, 2010. http://www.busse-yachtshop.de/.

———. „Raymarine C90W / C120W / C140W ‚Widescreen‘ bei Busse Yachtshop“, Dezember 20, 2010. http://www.busse-yachtshop.de/shop/wbc.php?sid=127232a9a982&tpl=produktdetail.html&pid=5223&recno=7.

Canada Gazette und Val. „Canada Gazette – Long-Range Identification and Tracking of Vessels Regulations“, Februar 3, 2011. http://www.gazette.gc.ca/rp-pr/p1/2009/2009-09-19/html/reg3-eng.html.

Conrad Electronic SE. „Bewegungsmelder 10 A, Serie 18“, Januar 18, 2011. http://www.conrad.de/ce/de/product/503144/IR-BEWEGUNGSMELDER-TYP-183182300000/0231043;jsessionid=FFEAC8093EDA52982AB3251692051475.ASTPCCP10.

———. „Druck-Sensoren-Sortiment im Conrad Online Shop“, Februar 3, 2011. http://www.conrad.de/ce/de/overview/0231110/Druck-Sensoren.

———. „Quadratische Lichtschranke Contrinex LLK-5050-003 Einweg-Lichtschranke (Empfänger) Reichweite 15000 mm im Conrad Online Shop“, Februar 3, 2011. http://www.conrad.de/ce/ProductDetail.html?hk=WW4&insert=V0&WT.mc_id=Froogle2&productcode=585404&utm_source=google&utm_medium=deeplink&utm_content=dl_article&utm_campaign=g_shopping.

Diehl BGT Defence. „Diehl BGT Defence | Sensoren“, November 8, 2010. http://www.diehl-bgt-defence.de/index.php?id=567.

Diehl BTG Defence. „SIMONE360“, 2010. http://www.diehl-bgt-defence.de/fileadmin/diehl-bgt-defence/upload/SIMONE360.jpg.

Donner, Michel, und Cornelis Kruk. „Supply Chain Security Guide“, 2009. http://siteresources.worldbank.org/INTPRAL/Resources/SCS_Guide_Final.pdf

Dührkop, Kai. Brief. „Preisanfrage passives Sonar“, März 11, 2011.

ELV Elektronik AG. „ABUS Lichtschranke LS 1020 | ELV-Elektronik“, Februar 3, 2011. http://www.elv.de/ABUS-Lichtschranke-LS-1020/x.aspx/cid_74/detail_10/detail2_22423/refid_GoogleBase.

Europäische Sicherheit. „Diehl Defence auf Wachstumskurs“. *Europäische Sicherheit*, Nr. 8 (2009). http://www.europaeische-sicher-heit.de/Ausgaben/2009/2009_08/Umschau/2009,08,umschau.html.

Federal Business Opportunities. „Predictive Analysis For Naval Deployment Activities (PANDA)“, April 18, 2006. https://www.fbo.gov/index?s=opportunity&mode=form&id=458c79831cef7f4e9c4862e37363f7aa&tab=core&tabmode=list&.

Fluke. „Ti 32 Wärmebildkamera für industrielle Anwendungen, Bauthermografie, Infrarotkamera - Fluke Deutschland“, Dezember 13, 2010. http://www.fluke.com/Fluke/dede/W%C3%A4rmebildkamera/Fluke-Ti32-%28Europe%29.htm?PID=56185.

Frankonia Handels GmbH & Co.KG. „Victory NV 5,6x62 T* von Zeiss - Nachtsichtgeräte - Optik - Frankonia.de“, Februar 2, 2011. http://www.frankonia.de/341898/126130/productdetail.html?lmEntry0=SEM&lmEntry1=BASE&ref=google_base#zeiss-nachtsichtgeraet-victory-nv-5-6x62-t-118931_341898.

Garcia, Mary Lynn. *Design and Evaluation of Physical Protection Systems*. 2nd Aufl. Amsterdam [u.a.]: Elsevier Butterworth-Heinemann, 2007.

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

Hoye, Gudrun K, Torkild Eriksen, Bente J Meland, und Bjorn T Narheim. „Space-based AIS for global maritime traffic monitoring“. *Acta Astronautica*, Nr. 62 (2006): 240-245.

International Maritime Organization. *SOLAS : Consolidated edition, 2009 consolidated text of the International Convention for the Safety of Life at Sea, 1974, and its Protocol of 1988 : articles, annexes and certificates Incorporating*. Consolidated ed., 2009 (5th ed.). London: IMO, 2009.

Issakov, Vadim. *Microwave Circuits for 24 GHz Automotive Radar in Silicon-based Technologies*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010. http://www.springerlink.com/content/tv17mq/#section=747247&page=4&locus=77.

Kathert, Beatrice. *Piraterie auf See*. Hamburg: Diplomica-Verl., 2010.

Knott, John. „The Paradox of Modern-day Piracy off Somalia: The dangers, and how to reduce them“, Februar 15, 2010. http://wp.hfw.com/the-paradox-of-modern-day-piracy-off-somalia-the-dangers-and-how-to-reduce-them/.

Kotte & Zeller GmbH. „Savana Nachtsichtgerät güstig online bestellen im Bushnell Nachtsichtgeräte Shop - Kotte & Zeller Online Store Versand preiswert kaufen“, Februar 2, 2011. http://www.kotte-zeller.de/Savana-Nachtsichtger%E4t.htm?websale7=kotte-zeller-shop&pi=12131&ref=froogle.

L-3 ELAC Nautik. „Multipurpose Sonar SUBEYE - Safety and Security for Mega Yachts and Cruise Ships“, 2010.

Markus, Till. „Die Regulierung anthropogener Lärmeinträge in die Meeresumwelt“. *Natur und Recht* 32, Nr. 4 (2010): 236-244.

National Research Council. *Autonomous Vehicles in Support of Naval Operations*. Wachington, D.C.: The National Academies Press, 2005.

http://books.nap.edu/openbook.php?record_id=11379&page=R1.
NauticExpo 2010. „OceanView Technologies Launches Apollo II HD, High Definition Thermal Camera - OceanView Technologies“, Dezember 13, 2010. http://news.nauticexpo.de/press/oceanview-technologies/oceanview-technologies-launches-apollo-ii-hd-high-definition-thermal-camera-32178-8904.html.
NewmanPaul. „Unmanned vehicles for schallow and coastal waters“, Januar 12, 2010.
Office of Naval Intelligence. „Horn of Africa: Threat Factors for Commercial Shipping and Forecast of Pirate Activity Through 2009“. Herausgegeben von Office of Naval Intelligence Piracy Team, 2009. http://www.marad.dot.gov/documents/Factors_Affecting_Pirate_Success_HOA.pdf.
Panagopoulos, S., und J.J. Soraghan. „Small-target detection in sea clutter“. *Geoscience and Remote Sensing, IEEE Transactions on* 42, Nr. 7 (2004): 1355-1361.
Ploch, Lauren, Christopher M. Blanchard, Rfonald O'Rourke, R. Chuck Mason, und Rawle O. King. „Piracy off the Horn of Africa“. Herausgegeben von Congressional Research Service, 2009. http://www.fas.org/sgp/crs/row/R40528.pdf.
Raytheon Anschütz. „Download Brochure: Small Target Tracker“. *Advanced Surveillance System*, November 11, 2010. http://www.raytheon-anschuetz.com/index.php?StoryID=229.
Raytheon. „High Frequency Surface Wave Radar (HFSWR)“, 2011. http://www.raytheon.com/capabilities/products/hfswr/.
Reichelt Elektronik. „BRESSER 5X50 DIG Optische Geräte, Ferngläser, Microskope, Teleskop - reichelt elektronik - Der Techniksortimenter - OnlineShop für Elektronik, Netbooks, PC-Komponenten, Kabel, Bauteile, Software & Bücher - ISO 9001:2000 Zertifiziert“, Februar 2, 2011. http://www.reichelt.de/?ARTICLE=92297;PROVID=2028.
———. „IRS 100 Alarmsensoren & Zubehör - reichelt elektronik - Der Techniksortimenter - OnlineShop für Elektronik, Netbooks, PC-Komponenten, Kabel, Bauteile, Software; Bücher - ISO 9001:2000 Zertifiziert“, Februar 3, 2011. http://www.reichelt.de/?ARTICLE=62378;PROVID=2028.
Remuss, Nina-Louisa. „Space Applications as a Supporting Tool for Countering Piracy – Outline for a European Approach“. Herausgegeben von ESPI European Space Policy Institute, 2010. http://www.espi.or.at/images/stories/ESPI_Report_29_online.pdf.
Rosenberg, David. „The Political Economy of Piracy in the South China Sea“. In *Piracy and Maritime Crime - Historical and Modern Case Studies*, herausgegeben von Bruce A Elleman, Abdrew Forbes, und David Rosenberg, 79-93. Newport, Rhode Island: Naval War College Press, 2010.
Seglermagazin.de. „Seglermagazin.de: Professionelle Wärmebildkameras werden bezahlbar“, April 19, 2007. http://www.seglermagazin.de/Professionelle-Waermebildkamer.4596.0.html.
shiploc.com. „ShipLoc - About ShipLoc“, 2011. http://www.shiploc.com/html/about_shiploc.html.
SPI GmbH. „SPI Marineshop“, Januar 14, 2011. http://www.spimarineshop.de/start.htm?d_TBY_AIS_CLA_AIS_CLASS_A_Transponder_COMAR.htm.

Umrechnung.org. „Universal Currency Converter™ Results“, November 16, 2010. http://www.xe.com/ucc/convert.cgi.

Urciuoli, Luca. „Supply chain security — mitigation measures and a logistics multi-layered framework“. *Journal of Transportation Security* 3 (2010): 1-28.

US Navy, Hrsg. „The Navy Unmanned Undersea Vehicle (UUV) Master Plan“, November 9, 2004. http://www.icrac.co.cc/Navy%20unmanned%20undersea%20masterplan.pdf.

Witherby Seamanship International Ltd, Hrsg. „BMP3 Best Management Practice 3 - Piracy off the Coast of Somalia and Arabian Sea Area“, Juni 2010. http://www.mschoa.org/bmp3/Documents/BMP3%20Final_low.pdf.

WolffChristian. „Radar Basics“. *Radartutorial.eu*, Dezember 13, 2010. http://www.radartutorial.eu/html/author.de.html.

Y-tronic Yacht-Electronic GbR. „Y-tronic Online Shop“, Dezember 20, 2010. https://www.shop.ck-software.de/webshop/index.php?korbid=70dc04018e74d6278c0c1375a8b4d7b7&shopid=7229&lang=&cur=EUR&rubrik=Antennenweichen%20Antennen%20und%20Kabel&refid=&refpw=&no_cache=81cdf4b74c6e77632d5782b0b1f59b24.