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

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

Thorsten Blecker / Thomas Will / Lutz Kretschmann

Indikatoren zur Bewertung der Selbstschutzfähigkeit von Schiffen bei Angriffen durch Piraten und Terroristen

PiraT-Arbeitspapiere zur Maritimen Sicherheit Nr. 17, Juli 2012

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.

Dr. Thomas Will studierte an der Universität Trier Wirtschaftsinformatik. Von 2006 bis 2011 arbeitete er als Wissenschaftlicher Mitarbeiter an der Technischen Universität Hamburg-Harburg. Nach erfolgreicher Promotion wechelte er zur Lufthansa Technik Logistik, wo er Großprojekte an der Schnittstelle zwischen Logistik und IT leitet. Zu seinen Forschungsthemen zählen: Automatisierung in der Containerlogistik, Informationstechnologien in der Logistik, AutoID / RFID, serviceorientierte Architekturen, Multi-Agenten-Systeme, Anti-Terror-Compliance und Supply Chain Security.

Dipl.- Ing. oec. Lutz Kretschmann studierte Wirtschaftsingenieurwesen an der Technischen Universität Hamburg-Harburg. Aktuell arbeitet er als Wissenschaftlicher Mitarbeiter am Fraunhofer-Center für Maritime Logistik und Dienstleistungen CML in Hamburg. 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. Für Inhalt und Aussage der Beiträge sind jeweils die entsprechenden Autoren verantwortlich. Nachdruck, auch auszugsweise, nur mit Genehmigung des IFSH.

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 pose a threat to maritime security. While the impact on the economy is still marginal, the financial risk for the individual vessel owner can be significant (Mildner & Groß 2010, S.27). This induces the need for a thorough risk management process carried out by the affected entities, resulting in suitable strategies of how to handle the given risks.

In a first step of risk management, a risk assessment is carried out, i.e. threats that pose a risk are identified and evaluated regarding their magnitude. The magnitude of a risk is characterized by (1) the threat level determined by the intent and capability of potential adversaries which constitute the likelihood of a risk bearing event occurring, (2) the vulnerability of the hit system which affects the likelihood of the attack being successful and (3) the severity of adverse effects on the system associated with the occurrence of an event (Haimes 2006, S.293). After identifying and evaluating risks with regard to their extent, suitable strategies of how to cope with them are developed. Possible strategies include the avoidance of a risk by the adjustment of shipping routes, the transfer through a suitable insurance or the reduction with an implementation of technological measures that decrease the vessel's vulnerability.

This paper contributes to a successful risk management of events associated with piracy and maritime terrorism. Firstly the risk-assessment process is outlined and adapted to the context of piracy and maritime terrorism. This constitutes the framework of this research, where a methodology is developed that enables the evaluation of a vessel's vulnerability towards a specific threat scenario. It is argued, that a vessel's vulnerability is characterized by its ability to (1) detect, (2) delay and (3) respond to an attack. Within the developed concept each of these characteristics is illustrated by a specific indicator. Together they form the vulnerability-indicator. A methodology that enables the qualitative measurement of these respective indicators is designed and implemented for one possible threat scenario: the boarding of a vessel by adversaries in the open sea. It consists of a set of five point scales, one adapted to each of the indicators, and influencing factors that are of relevance when rating a vessel within each particular scale. In order to verify the methodology, ensure its practical feasibility and the relevance of the identified influencing factors a number of expert interviews were conducted. Lastly the concept is applied to three hypothetical vessels in order to illustrate the procedure when evaluating a vessel's vulnerability.

The developed concept allows the measurement of a vessel's vulnerability according to a number of different dimensions. Thus, it contributes to the determination of the magnitude of risk associated with a specific threat scenario. By revealing potential weaknesses regarding certain threat scenarios, it also facilitates the implementation of technological and operational measures that efficiently reduce the likelihood of a successful attack on the vessel.

Abkürzungsverzeichnis

Abb.	Abbildung
bzw.	Beziehungsweise
CI	Composite-Indicator
etc.	et cetera
OECD	Organisation for Economic Co-operation and Development
PPS	Physical Protection System
u. a.	und andere
UN WWAP	United Nations World Water Assessment Programme
VLCC	Very Large Crude Carrier
z.B.	zum Beispiel

Abbildungs-, Tabellen- und Formelverzeichnis

Abbildungen

Tabellen

Formeln

1. Einleitung

Piraterie als Bedrohung für den Seehandel

Dieses Arbeitspapier entwickelt ein Indikatorenmodell zur Bewertung der Verwundbarkeit bzw. Selbstschutzfähigkeit von Schiffen bei Angriffen durch Piraten und maritime Terroristen. Gegenwärtig erlebt das Phänomen der Piraterie, unter dem im Kontext dieser Untersuchung ein Überfall auf ein Schiff mit dem Ziel der materiellen Bereicherung verstanden wird, [1] ein Comeback. [2] Seit einigen Jahren ziehen insbesondere die Vorfälle von Piraterie in den Gewässern vor Somalia eine verstärkte mediale Aufmerksamkeit auf sich. Die gegenwärtige Verschärfung der Situation spiegelt sich in einer aktuellen Befragung der maritimen Wirtschaft wider bei der 86% der befragten Reeder angeben, dass sich die Probleme in Bezug auf Piraterie in den vergangenen 12 Monaten vergrößert haben und 34% der befragten Reeder in der Vergangenheit bereits Opfer eines Piratenangriffes geworden zu sein (PWC 2011, S.21). Eine im Rahmen des PiraT Projektes durchgeführte Befragung von Reedern und deutschen Transportversicherern stützt diese Ergebnisse (Engerer & Gössler 2011a, S.11; Engerer & Gössler 2011b, S.13–14).

Maritimer Terrorismus als Bedrohung für den Seehandel

Ein weiteres Problem für die Seehandelssicherheit stellen Anschläge durch Terroristen im maritimen Umfeld dar. Entsprechende Angriffe auf Schiffe - zur Verursachung von größtmöglichem Schaden - sind vergleichsweise selten, sodass die Bedrohung weniger präsent ist.[3] Verglichen mit der Gefahr durch Piraten wird die Gefahr des maritimen Terrorismus durch Reeder und Transportversicherer als geringer eingeschätzt (Engerer & Gössler 2011a, S.11; Engerer & Gössler 2011b, S.13–14). Gleichzeitig bringen Bedrohungsszenarien des maritimen Terrorismus ein erhebliches Schadenspotential sowie eine enorme Symbolwirkung mit sich. Sie sollten dementsprechend, trotz einer augenscheinlich untergeordneten Bedrohungslage, nicht aus dem Fokus einer umfassenden Sicherheitsdebatte geraten (Geise 2007, S.9). Weiter ist festzustellen, dass terroristische Angriffe auf Schiffe und Häfen in den vergangenen zehn Jahren merklich zugenommen haben (McNicholas 2008, S.248). Schneider (2011, S.29–30) bestätigt einen solchen generellen Aufwärtstrend.

Bedrohungen stellen ein bedeutendes finanzielles Risiko für einen Reeder dar

Überfälle und Angriffe auf ein Schiff im Zusammenhang mit Piraterie und maritimem Terrorismus stellen aus unternehmerischer Sicht ein bedeutendes finanzielles Risiko dar. Die möglichen Folgen eines Vorfalls umfassen beispielsweise die Beschädigung oder den Gesamtverlust von Schiff und Ware, einen Wertverlust der Ware aufgrund verzögerter Lieferung, Vertragsstrafen wegen Lieferverzuges, Einnahmeausfälle oder etwaige Lösegeldzahlungen durch die Reederei (Mildner & Groß 2010, S.24,25,27). Hinzu kommen psychische und physische Belastungen von Betroffenen, welche im Zuge eines Angriffs entstehen. Für einen Reeder besteht die Notwendigkeit eines geeigneten Umgangs mit diesen Risiken im Rahmen eines Risikomanagementprozesses.

---

1 Eine Darstellung und Diskussion der Definition von Piraterie nach dem Seerechtsübereinkommen findet sich bei König u. a. (2011).

2 Eine Analyse zeitgenössischer Piraterie findet sich bei Petretto (2011).

3 Zu einer Diskussion von Kontext und Definition des Phänomens Maritimer Terrorismus sei verwiesen auf Schneider (2011).

Zunächst gilt es dabei als Teil des Risiko-Assessments zu identifizieren, welche Bedrohungen unter den betrachteten Phänomenen bestehen. Für diese Bedrohungsszenarien wird anschließend bewertet, wie hoch das jeweilige Risiko ist. Dazu werden die Risikoelemente Gefährdung, Verwundbarkeit und Auswirkungen ermittelt, aus denen sich das Bedrohungsniveau insgesamt ableiten lässt. Die Gefährdung gibt die Wahrscheinlichkeit eines Angriffes für ein bestimmtes Bedrohungsszenario an. Die Verwundbarkeit (Vulnerabilität) beschreibt, wie verletzbar das Objekt „Schiff“ gegenüber Angriffen durch Piraten und maritime Terroristen ist. Die Auswirkungen stellen die Folgen eines aus der Sicht der Piraten bzw. maritimen Terroristen erfolgreich durchgeführten Angriffs dar.

Risiko-Assessment identifiziert und bewertet bestehende Bedrohungen

Sind die Bedrohungen charakterisiert und bewertet, kann ausgehend hiervon eine geeignete Strategie zur Risikosteuerung gewählt werden. Es bestehen eine Reihe verschiedener Strategien für einen Reeder. Im Fokus dieser Untersuchung steht die Strategie der Risikoreduktion durch Implementieren von zur Sicherheit beitragenden Technologien an Bord eines Schiffes. Mit dem Einsatz geeigneter Technologien verringert sich die Wahrscheinlichkeit eines erfolgreichen Angriffes auf das Schiff und damit die Verwundbarkeit dieses Schiffes gegenüber einer Bedrohung.

Risikosteuerung ist anhand verschiedener Strategien möglich

Um einen Beitrag zu einem effektiven und effizienten Risikomanagement von Bedrohungen im Zusammenhang mit Piraterie und maritimem Terrorismus zu leisten, untersucht das vorliegende Arbeitspapier zunächst die relevanten Schritte des Risiko-Assessment. Dies bildet die Grundlage für die im folgenden Teil des Arbeitspapieres vorgenommene Untersuchung der Vulnerabilität eines Schiffes. Ziel ist es, die Vulnerabilität mithilfe eines qualitativen Indikators messbar zu machen. Hierzu wird ein allgemeingültiges Indikatorenkonzept entwickelt, welches auf die verschiedenen Bedrohungsszenarien, die im Zusammenhang mit Piraterie und maritimem Terrorismus existieren, anwendbar ist. Dieses Konzept wird für eine Gruppe von Bedrohungsszenarien ausgearbeitet. Anknüpfend durchgeführte Experteninterviews validieren das entwickelte Konzept hinsichtlich seiner praktischen Anwendbarkeit.

Ziel des Arbeitspapieres ist die (1) Darstellung des Risiko-Assessments sowie (2) die Entwicklung eines Vulnerabilitätsindikators

Der entwickelte Vulnerabilitätsindikator ermöglicht die Bewertung der Verwundbarkeit eines Schiffes in den identifizierten Bedrohungsszenarien anhand verschiedener Kriterien sowie die Identifikation der ursächlichen Schwachstellen. Er bildet die Grundlage für die in einem nächsten Schritt angestrebte Risikosteuerung durch die Auswahl geeigneter Technologien zur Reduktion der Verwundbarkeit eines Schiffes. Eine Zusammenstellung von zur Sicherheit beitragenden Technologien findet sich bei Blecker u. a. (2011a), Blecker u. a. (2011b) und Blecker u. a. (2012).

Der Vulnerabilitätsindikator ermöglicht es, ein Schiff hinsichtlich seiner Verwundbarkeit gegenüber verschiedenen Bedrohungen zu bewerten

2. Konzeptionelle und methodische Grundlagen

In einem ersten Schritt definiert das Kapitel „Konzeptionelle und methodische Grundlagen“ das Verständnis des Risikobegriffs und den Prozess des Risikomanagements. Weiter wird die Vorgehensweise zur Indikatorenentwicklung diskutiert und das Konzept des Physical Protection System vorgestellt. Dieses Konzept ist zentral für die Abbildung der Vulnerabilität, im Sinne der Verwundbarkeit eines Schiffes gegenüber den betrachteten Bedrohungen, in einem Indikator.

Konzeptionelle und methodische Grundlagen

2.1. Risiko und Risikomanagement

2.1.1. Risiko

Klassisches Risikoverständnis

In der Literatur finden sich verschiedene Interpretationen des Risikobegriffes. Die in einem spezifischen Zusammenhang verwandte Definition sollte dem jeweiligen Untersuchungsgegenstand angepasst sein (Böger 2010, S.11). Gemein ist den Interpretationen, dass sie Risiko als ein Maß der Wahrscheinlichkeit des Eintretens eines Ereignisses mit nachteiligen Auswirkungen auf ein System und der Intensität dieser Auswirkungen verstehen (Ehrhart u. a. 2011, S.63–64).[4] Entsprechende Ereignisse werden im Folgenden als Bedrohungen bezeichnet und in Bedrohungsszenarien beschrieben. Die klassische Herangehensweise versteht damit ein Risiko, wie in Formel 1 wiedergegeben, als Funktion abhängig von dem Schadensausmaß und der Eintrittswahrscheinlichkeit einer Bedrohung.

Formel 1: Klassische Risikofunktion

$$\text{Risiko}\ (\text{Schadensausmaß}, \text{Eintrittswahrscheinlichkeit})$$

Präzisierung der Risikoanalyse durch Einbeziehung qualitativer Faktoren

Anspruch des PiraT Projektes ist es, eine Präzisierung der maritimen Risikoanalyse zu ermöglichen (Ehrhart u. a. 2011, S.65). Hierzu soll die klassische Risikofunktion durch Einbeziehung qualitativer Faktoren erweitert werden.

Risikoverständnis dieser Untersuchung

Die diesem Arbeitspapier zugrunde gelegte Definition von Risiko orientiert sich am PiraT Risikomodell (Ehrhart u. a. 2011, S.65) und passt es, angelehnt an Haimes (2006, S.293,295), für die Untersuchung des zentralen Gegenstandes dieser Arbeit, der Verwundbarkeit eines Schiffes, an. Folgende Begriffserklärungen werden getroffen:

- **Risiko** resultiert aus einer **Gefährdung** für ein **vulnerables System** mit nachteiligen **Auswirkungen** auf das System.
- Eine **Gefährdung** besteht, wenn sowohl **Intention** als auch **Fähigkeit** gegeben sind, bei dem System eine Beeinträchtigung hervorzurufen.
- **Intention** ist gegeben, wenn ein Wille und eine Motivation das System anzugreifen, bestehen.
- **Fähigkeit** beschreibt das Leistungsvermögen das System anzugreifen und Beeinträchtigungen hervorzurufen.
- **Vulnerabilität** (im Sinn von Verwundbarkeit) beschreibt dem System innewohnende physische, technische, organisatorische und / oder kulturelle Eigenschaften, die bei einem Eintreten der Bedrohung determinieren, ob die Bedrohung Auswirkungen hat.
- **Auswirkungen** sind nachteilige Beeinträchtigungen im Sinne von Verletzungen und Schädigungen des Systems, die sich beim Eintreten einer Bedrohung ergeben.

[4] Die vorliegende Arbeit betrachtet keine spekulativen Risiken, die sowohl vorteilhafte als auch nachteilige Auswirkungen haben können. Diese Beschränkung resultiert aus der Tatsache, dass Betroffene bei einer Konfrontation mit den hier betrachteten Risiken auf den Schutz gegenüber nachteiligen Auswirkungen fokussieren (McGill 2008, S.19).

Wie in Formel 2 dargestellt wird Risiko verstanden als eine Funktion der einzelnen oben beschriebenen Risikoelemente Intention, Fähigkeit, Vulnerabilität und Auswirkung. Es wird ein positiver Zusammenhang zwischen den Risikoelementen und dem Risiko unterstellt: erhöht sich eins der Risikoelemente hat dies ein höheres Risiko zur Folge.

Formel 2: Risiko als Funktion einzelner Risikoelemente

$$\text{Risiko}\,(\text{Gefährdung}\,(\text{Intention, Fähigkeit}), \text{Vulnerabilität, Auswirkung})$$

Wird für diese Funktion eine explizite Definition vorgenommen, also festgelegt in welcher Weise die einzelnen Risikoelemente zum Risiko beitragen[5], ermöglicht dies eine Berechnung der Höhe des Risikos.

2.1.2. Risikomanagement

Risikomanagement

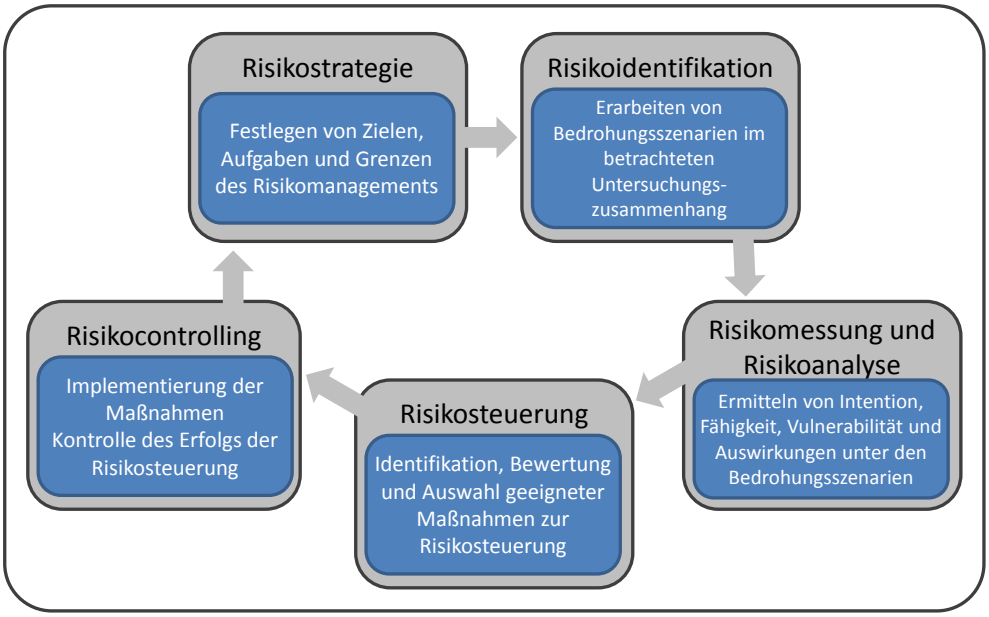
Die grundlegende Aufgabe des Risikomanagements besteht in dem Umgang mit Risiken oder der Behandlung dieser (Böger 2010, S.19). Nach der Definition des Deutschen Rechnungslegungs Standards Committee ist Risikomanagement ein „nachvollziehbares, alle Unternehmensaktivitäten umfassendes System, das auf Basis einer definierten Risikostrategie ein systematisches und permanentes Vorgehen mit folgenden Elementen umfasst: Identifikation, Analyse, Bewertung, Steuerung, Dokumentation und Kommunikation von Risiken sowie die Überwachung dieser Aktivitäten“ (Fiege 2006, S.58). Folglich muss das Risikomanagement, aufbauend auf einer Strategie, Risiken erfassen, bewerten, überwachen und spätestens, wenn sie zu einer ernsten Gefährdung werden, durch geeignete Maßnahmen steuern (Rosenkranz & Missler-Behr 2005, S.40).

Risikomanagementprozess

Die Umsetzung des Risikomanagements findet in einem Risikomanagementprozess statt. Abb. 1 stellt den Risikomanagementprozess als einen Rückkopplungsprozess, der die Schritte der Risikostrategie, Risikoidentifikation, Risikomessung und Risikoanalyse, Risikosteuerung sowie das Risikocontrolling beinhaltet, dar (Burger & Buchhart 2002, S.31; Rosenkranz & Missler-Behr 2005, S.41; Wolke 2009, S.3–5).

[5] Eine mögliche Funktion könnte die Multiplikation der einzelnen Risikoelemente darstellen. Soll eine Funktion unterstellt werden müssen die Einheiten der Funktionsparameter sowie die qualitative Natur einzelner Parameter Berücksichtigung finden.

Abb. 1: Risikomanagementprozess



Quelle: In Anlehnung an Rosenkranz & Missler-Behr (2005, S.40)

Risikostrategie

Die **Risikostrategie** bestimmt ausgehend von der strategischen Ausrichtung des Systems die Ziele, Aufgaben und Grenzen des Risikomanagements (GAO 2005, S.24). Besteht eine Diskrepanz zwischen Risikostrategie und tatsächlicher Risikosituation, muss die Risikostrategie oder die Risikosteuerung überdacht bzw. angepasst werden (Rosenkranz & Missler-Behr 2005, S.41).

Risiko Assessment

Risikoidentifikation, Risikomessung und Risikoanalyse stellen zusammengefasst das **Risiko-Assessment** dar. Hierbei gilt es zu klären (Kaplan & Garrick 1981, S.13):

1. welche negativen Ereignisse eintreten können: Identifikation möglicher Bedrohungsszenarien,
2. wie hoch die Wahrscheinlichkeit des Eintretens dieser Ereignisse ist: Bestimmung von Gefährdung und Vulnerabilität unter den Bedrohungsszenarien und
3. welche Auswirkungen sich als Folgen eines Eintretens ergeben: Bestimmung der Auswirkungen infolge des Eintretens der Bedrohungsszenarien.

Sind für denkbare Bedrohungsszenarien Intention und Fähigkeit des Angreifers ermittelt, die Vulnerabilität des angegriffenen Systems bestimmt und potentielle Auswirkungen eines Eintretens ausgemacht, können die Risiken im Rahmen der Risikoanalyse verglichen und diejenigen, von denen die größte Gefährdung für das System ausgeht, identifiziert werden. Ziel der Analyse ist es weiter zu ermitteln, ob bezüglich der identifizierten und gemessenen Risiken ein Handlungsbedarf besteht (Wolke 2009, S.5).

Risikosteuerung

Die **Risikosteuerung** umfasst die Identifikation von Maßnahmen, mit denen auf die identifizierten Risiken reagiert werden kann, deren Evaluation sowie eine Auswahl von Maßnahmen, welche umgesetzt werden sollen, um die Risiken zu beeinflussen. Mögliche Strategien der Risikosteuerung sind (Rosenkranz & Missler-Behr 2005, S.45-46, 283, 287-289; Wolf & Runzheimer 2009, S.89; Wolke 2009, S.79–101):

- Risikovermeidung als Ausschluss eines Risikos durch den Verzicht auf die risikobehaftete Handlung,
- Risikoreduktion als Verminderung des Risikos durch Einflussnahme auf das zugrundeliegende Ursache- und Wirkungssystem,
- Risikobegrenzung als Handlungsanweisung, Risiken nur bis zu einer festgelegten Grenze einzugehen,
- Risikoakzeptanz als wissentliches Akzeptieren und Tragen des Risikos sowie
- Risikoübertragung als Transfer des Risikos bzw. der mit dem Risiko verbundenen Folgen auf eine andere Partei.

Bei der Identifikation geeigneter Maßnahmen gilt es folgende Fragen zu beantworten (Haimes 2006, S.295):

1. Welche Formen der Risikosteuerung sind anwendbar?
2. Welche Abwägungen zwischen relevanten Kosten, Nutzen und Risiken gilt es zu berücksichtigen?
3. Wie wirken sich heutige Entscheidungen auf zukünftige Handlungsoptionen aus?

Risikocontrolling

Der Risikomanagementprozess wird abgeschlossen mit dem **Risikocontrolling**. Dieses umfasst das Implementieren der ausgewählten Maßnahmen sowie die Überwachung ihres Beitrages zu einer Verringerung des Risikos.

2.1.3. Qualitative und quantitative Risikomessung

Ansätze zur Risikomessung

Risiken, die auf Grund verschiedener Bedrohungen bestehen, können entweder mithilfe qualitativer oder quantitativer Ansätze gemessen werden.

Quantitative Risikoabschätzung

Im Idealfall findet eine quantitative Bestimmung des Risikos statt. Numerische Werte werden für die einzelnen Risikoelemente (Intention, Fähigkeit, Vulnerabilität und Auswirkung) ermittelt und mithilfe einer geeigneten Funktion zusammengefasst. Dies ermöglicht es, verschiedene Risiken in ihrer Verlusthöhe zu bestimmen und zwischen verschiedenen Risiken für ein Objekt zu vergleichen (Greenberg u. a. 2006, S.143). Des Weiteren ist es möglich, Risikosteuerungsansätze zur Verringerung des Risikos auf einer monetären Ebene hinsichtlich ihrer Kosten und ihres Nutzens zu bewerten, um zu berechnen, in welchen Bereichen wie viel Aufwand zur Verringerung des Risikos anfallen sollte.

Voraussetzungen der quantitativen Risikoabschätzung

Ein quantitativer Ansatz setzt voraus, dass sowohl eine Abschätzung der Wahrscheinlichkeit des Eintretens der Bedrohung – resultierend aus Intention und Fähigkeit – als auch eine Abschätzung der Erfolgswahrscheinlichkeit bei Eintreten der Bedrohung – im Sinne der Vulnerabilität – sowie eine wertmäßige Abschätzung der Auswirkungen vorgenommen wird. Diese quantitative Bestimmung ist möglich, aber aufwendig (Greenberg u. a. 2006, S.143). Ein Problem, insbesondere bei der Bestimmung der Wahrscheinlichkeiten im Zusammenhang mit terroristischen Bedrohungen, ist, dass keine statistischen Berechnungen der Wahrscheinlichkeiten anhand von Vergangenheitsdaten vorgenommen werden können (Willis u. a. 2007, S.5). Eine Alternative um Wahrscheinlichkeiten zu Gefährdung und Vulnerabilität zu ermitteln, ohne auf Vergangenheitsdaten zurückzugreifen, besteht beispielsweise in dem Einsatz von Bayes Modellen (Bayesian decision theory, Bayesian statistics) (Greenberg u. a. 2006, S.143;

Cox 2009, S.45). Hierbei werden ausgehend von Expertenbeurteilungen zu Gefährdung und Vulnerabilität die Wahrscheinlichkeiten abgeleitet.

Qualitative Risikoabschätzung

Sind die Informationen zur Realisierung einer quantitativen Risikoabschätzung im Sinne von Vergangenheitsdaten nicht verfügbar bzw. wird der Aufwand zur Ermittlung der Ausprägungen der Risikoelemente als nicht gerechtfertigt angesehen oder sind qualitative Einschätzungen im Untersuchungszusammenhang als ausreichend zu betrachten, kann ein qualitativer Ansatz gewählt werden. Auch wenn auf Grundlage der qualitativen Erkenntnisse keine Aussage über den absoluten Aufwand, der in die Risikosteuerung einfließen sollte, getroffen werden kann, so ist es doch möglich, die Risiken in ihrem Ausmaß miteinander zu vergleichen. Daraus lässt sich eine Priorisierung von Bedrohungen, die es mithilfe geeigneter Risikosteuerungsmaßnahmen zu beeinflussen gilt, ableiten. Mit anderen Worten: eine qualitative Analyse des Risikos kann nicht ermitteln wie viel Geld in welche Risikosteuerungsansätze investiert werden sollte, aber sie kann helfen, die Frage zu beantworten, welche Priorität verschiedene Bedrohungen bei der Risikosteuerung einnehmen sollten (Greenberg u. a. 2006, S.143–144).

Skalen zur qualitativen Risikoabschätzung

Bei einer qualitativen Bestimmung von Risiken werden die Risikoelemente Gefährdung, Vulnerabilität und Auswirkungen in ihrer Ausprägung anhand von sprachlichen Ausformulierungen (beispielsweise hoch, mittel, niedrig) oder quantifizierten Skalen (beispielsweise von 1 bis 10) eingeordnet (RAMCAP 2006, S.65). Die einzelnen Stufen dieser Skalen müssen adäquat beschrieben sein, um eine sinnvolle und richtige Zuordnung zu ermöglichen (Fletcher 2005, S.1577). Bei Skalen, die eine Wahrscheinlichkeit abbilden, können den einzelnen Stufen auch Wahrscheinlichkeitsbereiche (beispielsweise 20-50 %) zugeordnet werden (Bartlett 2004, S.98). Die Abschätzung der Ausprägung der Risikoelemente unter einer Bedrohung anhand der Skalen muss von Experten vorgenommen werden. Das resultierende Risiko ermittelt sich anhand einer geeigneten Zusammenfassung der einzelnen Risikoelemente.

2.2. Indikatoren und Indikatorenentwicklung

2.2.1. Indikatoren

Definition eines Indikators

Um die Funktion eines Indikators zu erfassen, folgt zunächst eine Definition. Der Begriff des Indikators wird in der Literatur von verschiedenen Autoren unterschiedlich definiert (Birkmann 2006, S.57). Die hier verwendete Definition orientiert sich an der von Gallopin (1997):

> Ein Indikator ist ein Kennzeichen, das relevante Informationen in Bezug auf ein betrachtetes Phänomen, dem Indikandum, zusammenfasst. Das eigentliche Interesse gilt dabei dem Indikandum als einem nicht direkt messbaren und oftmals komplexen Sachverhalt bzw. Zustand und dessen Zustandsveränderung.

Folglich sind Indikatoren Variablen, die eine funktionale Darstellung eines Merkmals, etwa der Qualität und / oder einer Eigenschaft eines Objektes oder Systems ermöglichen. Der Indikator muss dabei eine hinreichende Konkretisierung des Indikandums zulassen (Birkmann 1999, S.121).

Formen von Indikatoren

Indikatoren können entweder qualitative nominale Variablen, ordinale Variablen oder quantitative Variablen sein. Sind keine quantitativen Daten verfügbar, oder ist die betrachtete Eigenschaft nicht quantifizierbar, muss auf qualitative Indikatoren zurückgegriffen werden. Qualitative Indikatoren sind quantitativen vorzuziehen, wenn mit der Erhebung von quantitativen Daten ein unverhältnismäßig hoher Aufwand verbunden ist (Gallopin 1997).

Funktionen von Indikatoren

Allgemein sind Indikatoren Werkzeuge, welche die Charakteristika komplexer Zusammenhänge in einer transparenten Weise beschreiben und operationalisieren. Sie dienen als Brücke zwischen theoretischen Modellen komplexer Systeme und einer praktischen Entscheidungsfindung. Die Funktionen, die ein Indikator in diesem Zusammenhang erfüllen kann, sind (Gallopin 1997):

- Beurteilung des Zustandes und der Entwicklung eines Objekts oder Systems.
- Vergleich des Zustandes mehrerer Objekte oder Systeme untereinander.
- Bewertung des Zustandes eines Objektes oder Systems und dessen Entwicklung in Relation zu festgelegten Zielen.
- Bereitstellung von Warnhinweisen.
- Antizipation zukünftiger Zustände und Entwicklungen.

Damit erlauben Indikatoren vergleichende Analysen, Benchmarking sowie die Unterstützung von Entscheidungsträgern in komplexen Entscheidungssituationen (Hiete & Merz 2009, S.3).

Schlüsselrolle von Indikatoren bei der Bewertung der Vulnerabilität

Indikatoren finden verbreitet Anwendungen im Kontext ökonomischer, gesellschaftlicher und ökologischer Analysen (Hiete & Merz 2009, S.3). Weithin akzeptiert sind etwa Indikatoren wie das Bruttoinlandsprodukt oder die Arbeitslosenquote, wenn es darum geht, die konjunkturelle Lage und Entwicklung eines Landes (in diesem Zusammenhang das Indikandum) darzustellen (Birkmann 2006, S.58). Eine Schlüsselrolle nehmen Indikatoren bei der Bewertung der Vulnerabilität eines Objektes oder Systems ein. Darauf aufbauend werden Bewältigungskapazitäten und Bewältigungsstrategien zur Verringerung der Vulnerabilität entwickelt (Birkmann 2006, S.56). In diesem Zusammenhang zeigen Indikatoren die Anfälligkeit, Bewältigungskapazität und Widerstandsfähigkeit eines Systems gegenüber einer Bedrohung an (Birkmann 2006, S.57). Die Vulnerabilität eines Systems ist im Allgemeinen determiniert durch eine Reihe verschiedener Faktoren. Folglich kann sie selten durch einen einzigen Indikator, sondern muss vielmehr mithilfe von multidimensionalen Konzepten, wie Composite-Indicators (CI) (composite: englisch für zusammengesetzt) abgebildet werden (Hiete & Merz 2009, S.3).

2.2.2. Zusammengefasste Indikatoren

Zusammengefasste Indikatoren – Composite Indicators

Werden in einem Indikator mehrere Einzelindikatoren zu einem einzigen Wert integriert, handelt es sich um einen zusammengefassten Indikator oder CI. CI eignen sich aufgrund der Aggregation besonderes gut, um komplexe Probleme darzustellen und mehrere betrachtete Objekte miteinander zu vergleichen (OECD 2008, S.13).

Die Aggregation der einzelnen Indikatoren findet anhand eines zugrundeliegenden theoretischen Modelles statt. Aus diesem Modell geht hervor, welche Einzelindikato-

ren warum in den CI aufgenommen werden und wie ihre Gewichtung bei der Aggregation ausfällt. Das Modell bildet den untersuchten Zusammenhang anhand passender Parameter auf einem abstrakten, oftmals vereinfachten Niveau, ab. Die Gewichtung repräsentiert die relative Bedeutung der einzelnen Indikatoren im untersuchten Zusammenhang.

Problem der Subjektivität von Composite Indikators

Dabei unterliegen die Auswahl von Modell und Gewichtung genauso wie die Behandlung von fehlenden Werten einer subjektiven Entscheidung (Cherchy u. a. 2006, S.1). Für CI folgt daraus, dass ihre Aussagekraft entscheidend von den subjektiv getroffenen Bewertungen abhängt. Deshalb sind Manipulation oder Verfälschung und dadurch realitätsfernen Ergebnisse möglich. Ein entscheidender Schritt bei der Erstellung von CIs ist deshalb, die Quellen von Subjektivität zu identifizieren, getroffene Entscheidungen genau zu validieren, sowie dahingehend zu untersuchen, ob sie zu einer Verfälschung der aggregierten Ergebnisse beitragen (Cherchy u. a. 2006, S.1). Ob ein theoretisches Modell geeignet ist, den untersuchten Zusammenhang abzubilden, kann nur über die Akzeptanz des Modells durch Experten überprüft werden (Saltelli 2006, S.69).

Vor- und Nachteile von Composite Indikators

In der Literatur gibt es geteilte Meinungen darüber, ob es sinnvoll ist, Einzelindikatoren zu einem CI zusammenzufassen. Ein CI kann aussagekräftige und bedeutungsvolle Information über die Realität abbilden, die über eine Nebeneinanderstellung der Einzelindikatoren hinausgeht. Außerdem ist ein einzelner zusammengefasster Wert äußerst nützlich um ein öffentliches Interesse zu erzeugen und so die Aufmerksamkeit von Entscheidungsträgern auf eine Fragestellung zu lenken. Gegen die Verwendung von CI spricht die Subjektivität der Gewichtung der Einzelindikatoren bei der Aggregation, wodurch der CI an Aussagekraft verliert (Sharpe 2004, S.5).

2.2.3. Indikatorenentwicklung

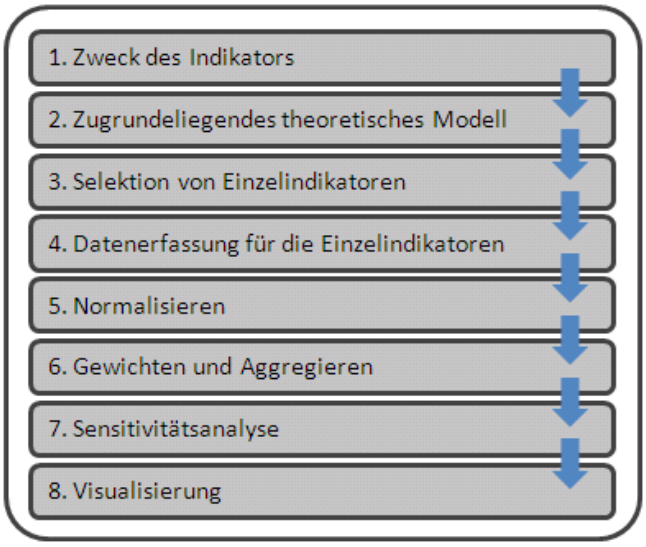
Prozess der Indikatorenentwicklung

Die Entwicklung eines Indikators muss systematisch, transparent und verständlich sein, wobei der Prozess in eine Reihe von iterativen Schritten aufgeteilt ist. In der Literatur finden sich Prozesse für die Indikatorenentwicklung unter anderem bei Maclaren (1996), UN WWAP[6] (2003, S.41–46), Brikmann (2006, S.63–64), OECD[7] (2008, S.19–21) und Hiete & Merz (2009, S.3–7). Inhaltlich ähneln sich die Vorgehensweisen. Abb. 2 stellt den im Folgenden erläuterten Prozess dar, der sich an dem von Hiete & Merz (2009, S.3–7) orientiert.

[6] United Nations World Water Assessment Programme (UN WWAP).

[7] Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (englisch Organisation for Economic Co-operation and Development) (OECD).

Abb. 2: Schritte der Indikatorenentwicklung



(1) Zweck des Indikators

Der erste Schritt der Indikatorenentwicklung legt fest, welcher Informationsbedarf durch den Indikator abgedeckt werden soll und welches Ziel mit den gewonnenen Informationen verfolgt wird. Dies bestimmt den **Zweck des Indikators** und bildet die Basis für die Auswahl des Indikandums als dem Phänomen oder Sachverhalt von Interesse (Birkmann 2006, S.59). Der Zweck des Indikators bestimmt maßgeblich die weiteren Schritte der Indikatorenentwicklung.

(2) Theoretisches Modell das dem Indikator zugrunde liegt

Die Suche nach einem aussagekräftigen und stimmigen konzeptionellem **theoretischen Modell,** das eine Abbildung des Indikandums ermöglicht, ist der Ausgangspunkt der eigentlichen Entwicklung des Indikators. Das Modell bildet die Grundlage des Indikators und muss mit entsprechender Sorgfalt ausgesucht werden. Ein konzeptionelles Modell ist eine verbale oder visuelle Abbildung eines Zusammenhangs aus der realen Welt auf abstraktem Niveau. Es muss das untersuchte Phänomen klar beschreiben und verschiedene Aspekte, sowie deren Beziehungen, abbilden (OECD 2008, S.22). Wie bei jedem Modellbildungsprozess ist eine Abwägung zwischen Genauigkeit und Vereinfachung zu treffen. Auf der einen Seite müssen die theoretischen, unter Umständen komplexen Zusammenhänge des betrachteten Sachverhaltes abgebildet werden, auf der anderen Seite sollte die Anzahl der mit einbezogenen Einflussfaktoren nicht zu groß werden. Es muss sichergestellt sein, dass alle für den untersuchten Zusammenhang entscheidenden Aspekte abgebildet sind und gleichzeitig das konzeptionelle Modell nachvollziehbar bleibt (Hiete & Merz 2009, S.4).

(3) Selektion von Einzelindikatoren

Ein Indikator kann nur so gut sein, wie die Summe der Einzelindikatoren. Mit entsprechender Sorgfalt ist im dritten Schritt bei der **Selektion von Einzelindikatoren** vorzugehen (OECD 2008, S.23). Den Rahmen für die Auswahl von Einzelindikatoren bildet das konzeptionelle Modell. Die hier dargestellten Aspekte gilt es mithilfe von passenden Einzelindikatoren zu erfassen und wiederzugeben. Entscheidende Kriterien bei dieser Auswahl sind Relevanz, Genauigkeit, Aktualität, Verfügbarkeit, Interpretierbarkeit und Kohärenz (OECD 2008, S.46–48).

Nach der Selektion folgt die **Datenerfassung für die Einzelindikatoren**. Dabei gilt es präzise, zuverlässige und zugängliche Daten zusammenzutragen, die entweder bereits verfügbar sind, oder neu erhoben werden.

(4) Datenerfassung für die Einzelindikatoren

Liegen die Einzelindikatoren in voneinander abweichenden Einheiten vor und sollen zu einem CI zusammengefasst werden, ist der nächste Schritt der Indikatorenentwicklung eine **Normalisierung**. Eine Aufzählung verschiedener Vorgehensweisen zur Normalisierung findet sich bei OECD (2008, S.30). Durch das Normalisieren ist es möglich sowohl quantitative als auch qualitative Einzelindikatoren in ein Modell zu integrieren da sie im Anschluss in derselben Einheit vorliegen (Hiete & Merz 2009, S.7).

(5) Normalisierung der Einzelindikatoren

Liegen alle Einzelindikatoren in Folge der Normalisierung in derselben Einheit vor, folgt das **Gewichten und Aggregieren** zu einem CI. Die Gewichtung spiegelt den Beitrag der Einzelindikatoren zur Erklärung des betrachteten Phänomens bzw. ihre relative Bedeutung innerhalb des konzeptionellen Modells wider. Es gibt eine Reihe verschiedener Verfahren für die Gewichtung. Die simpelste ist eine einfache Addition[8] der Einzelindikatoren. Dabei kommt es zu dem unerwünschten Effekt, dass eine volle Kompensation von geringen Werten bei einigen Einzelindikatoren durch hohe Werte bei anderen Einzelindikatoren möglich ist. Dieser Effekt ist bei einer geometrische Aggregation[9] der Daten teilweise aufgehoben.[10] Ein Multi-Criteria Approach, wie er bei OECD (2008, S.112–115) beschrieben ist, schließt ihn komplett aus. Bei den meisten CI gehen alle Einzelindikatoren mit dem gleichen Gewicht ein (OECD 2008, S.31).

(6) Gewichten und Aggregieren der Einzelindikatoren

Der Prozess der Indikatorenentwicklung verlangt in verschiedenen Schritten subjektive Einschätzungen durch den Modellbildenden. Dies umfasst die Auswahl der Einzelindikatoren, den Umgang mit fehlenden Werten, die Wahl der Normalisations- und Aggregationsmethode sowie die Gewichtung der Einzelindikatoren (OECD 2008, S.117). Diese Subjektivität macht die Aussagekraft des Indikators anfechtbar selbst wenn Annahmen und Einschätzungen in transparenter Weise von einem Expertengremium getroffen wurden. Aufgabe der **Sensitivitätsanalyse** ist es darzustellen, wie sich die subjektiv getroffenen Annahmen auf den Indikator auswirken. So kann zwar nicht die Subjektivität an sich vermieden werden, aber es ist möglich darzustellen, wie groß der Einfluss verschiedener subjektiver Einschätzungen auf den Indikator ist.

(7) Sensitivitätsanalyse

Die in einem Indikator zusammengefassten Informationen sollen Entscheidungsträgern oder anderen Endnutzern übersichtlich zugänglich gemacht werden. Dazu findet im letzen Schritt der Indikatorenentwicklung eine **Visualisierung** der Ergebnisse statt. Tabellen, auch wenn sie die kompletten Informationen zur Verfügung stellen, können dabei unübersichtlich und weniger zugänglich sein als Grafiken (OECD 2008, S.40). Die Form der Präsentation wird entsprechend der Zielgruppe und des verfolgten Zweckes gewählt.

(8) Visualisierung des Indikators

---

8 Das verbreiteteste Verfahren der linearen Aggregation ist die Summation gewichteter und normalisierter Einzelindikatoren. Siehe hierzu OECD (2008, S.103).

9 Bei der geometrischen Aggregation werden die Einzelindikatoren über eine Multiplikation zusammengefasst. Siehe hierzu OECD (2008, S.104).

10 Beispiel: Zwei Objekte mit Einzelindikatoren von (21,1,1,1) und (6,6,6,6) haben bei einfacher additiver Aggregation und gleicher Gewichtung der Einzelindikatoren beide einen CI von 6. Bei geometrischer Aggregation haben die Objekte einen CI von 2,14 bzw. 6 (OECD 2008, S.104).

2.3. Physical Protection System

Konzept des Physical Protection System

Das hier vorgestellte Konzept des Physical Protection System (PPS) wurde von den Sandia National Laboratories für den Schutz von nuklearen Anlagen entwickelt. Die im Folgenden beschriebenen Funktionen des PPS sowie die Methodik, mit der sich ein PPS entwerfen und analysieren lässt, sind von Garcia (2007; 2006) übernommen.

Physical Protection System stellt die Security eines Objektes bereit

Aufgabe eines PPS ist die Gewährleistung von Sicherheit, im Sinne von Security, für ein Objekt. Dabei integriert das PPS Menschen, Prozesse, elektronische und physische Komponenten zum Schutz des Objektes (Garcia 2007, S.1). Bei den Objekten kann es sich um Personen, Eigentum, Informationen oder jede andere Form von Besitz, dem ein Wert zugeschrieben wird, handeln (Garcia 2006, S.2). Ziel ist, diese gegen offene oder verdeckte böswillige Handlungen zu schützen oder die Durchführung der Handlungen im Vorfeld durch ein Abschrecken zu verhindern. Typische böswillige Handlungen, im Sinne von möglichen Bedrohungen für das Objekt, sind Sabotage von kritischem Equipment, Diebstahl von Eigentum oder Informationen sowie Verletzen von Menschen (Garcia 2006, S.35). Im Kontext einer Risikobetrachtung bestimmt das PPS maßgeblich die Vulnerabilität des Objektes gegenüber diesen Bedrohungen.

Funktionen eines PPS

Um den Schutz eines Objektes zu gewährleisten, erfüllt das PPS die Funktionen: Detektion eines Angriffs, Verzögerung des Angriffs und Reaktion auf den Angriff.

Detektionsfunktion

Die **Detektionsfunktion** hat die Aufgabe, ein unerlaubtes Eindringen einer Person, eines Fahrzeuges oder eines Gegenstandes in den durch das PPS geschützten Bereich zu erkennen und eine angemessene Reaktion zu initiieren (Garcia 2006, S.83). An der Detektion eines Eindringens können verschiedene Sensorsysteme (zum Beispiel (z.B.) Videoüberwachungssysteme) sowie vor Ort befindliches Wach- oder Betriebspersonal beteiligt sein. Für die Leistungsbewertung der Detektionsfunktion sind die Wahrscheinlichkeit einen Angriff zu detektieren, die Zeit, welche Alarmbewertung und Initiierung der Reaktion in Anspruch nehmen, sowie die Fehlalarmquote entscheidend (Garcia 2007, S.65).

Verzögerungsfunktion

Die **Verzögerungsfunktion** des PPS beinhaltet Elemente, welche das Eindringen eines Angreifers in den geschützten Bereich behindern, und so die benötigte Zeit des Eindringens und den zu treibenden Aufwand des Eindringenden erhöhen. Nur wenn das Vorankommen eines Angreifers lange genug verzögert werden kann, bleibt nach einer Detektion genug Zeit für eine rechtzeitige Umsetzung einer Reaktion am Ort des Angriffs. Durch das Erhöhen des Aufwandes eines Angriffs haben die Verzögerungselemente außerdem die Wirkung wenig entschlossene Angreifer von einem Angriff abzuschrecken. Typische Verzögerungselemente eines PPS sind strukturelle Barrieren (Zäune, Mauern, Stacheldraht, verstärkte Wände und Türen oder Fahrzeugsperren), disponierbare Barrieren (die ein Fortkommen behindern etwa Gitter, rutschiger oder klebriger Schaum und solche, die die Sinneswahrnehmung beeinträchtigen etwa Rauch, Reizgas oder Verdunkelung) und Wachpersonal (Garcia 2006, S.232; Garcia 2007, S.220). Für die Leistungsbewertung der Verzögerungsfunktion ist die Zeit, die nötig ist, die Hindernisse zu überwinden, maßgeblich (Garcia 2007, S.65).

Reaktionsfunktion

Reaktion ist die dritte Funktion des PPS. Es besteht ein weites Spektrum an Handlungsoptionen, mit denen auf eine Sicherheitsverletzung reagiert werden kann. Eine angemessene Reaktion hängt ab von der Art der Bedrohung, den Konsequenzen ei-

nes erfolgreichen Angriffs, dem Wert des gesicherten Objektes, anderen Risikomanagementalternativen für das Objekt, dem Level an Risikotoleranz sowie rechtlichen Erwägungen (Garcia 2006, S.237).

Unmittelbare Reaktion

Die Reaktion unterteilt sich in eine unmittelbare Vor-Ort-Reaktion und eine nachträgliche verzögerte Reaktion (Garcia 2007, S.243). Eine unmittelbare Reaktion besteht in einem rechtzeitigen Aufbieten von internem oder externem (etwa Polizei- oder private Sicherheitskräfte) Sicherheitspersonal in ausreichender Stärke am Ort des Angriffs. Aufgabe des Sicherheitspersonals ist es, den Angriff zu neutralisieren. Dies ist erreicht, wenn der Angreifer sich freiwillig ergibt oder nicht mehr in der Lage ist, seinen Angriff fortzuführen. Ausschlaggebend für ein erfolgreiches Neutralisieren sind neben einer ausreichenden Anzahl von Sicherheitskräften auch Training, Taktik und ihre Ausrüstung (Garcia 2006, S.238). Darüber hinaus sind eine präzise Kommunikation der Bedrohung und Koordination der Sicherheitskräfte entscheidend (Garcia 2006, S.238). Die Leistungsbewertung einer unmittelbaren Reaktion findet anhand der Zeit bis zum Eintreffen der Sicherheitskräfte und deren Aussicht auf ein erfolgreiches Neutralisieren des Angriffes statt.

Verzögerte Reaktion

Eine verzögerte Reaktion ist dann sinnvoll, wenn das Unterbinden des Angriffs weniger bedeutend ist als ein Wiederanlaufen des Betriebs im Anschluss an den Angriff. Beispiele für eine verzögerte Reaktion sind ein Durchsehen von Überwachungsvideos, Aufspüren und Zurückgewinnen von entwendeten Gütern oder eine strafrechtliche Verfolgung des Angreifers (Garcia 2006, S.238).

Konzeption und Bewertung eines PPS

Bei der Konzeption und Bewertung eines PPS ist entscheidend was das PPS zu leisten im Stande ist nicht wie es auf einen möglichen Angreifer - im Sinn eines Abschreckens - wirkt. Eine mögliche Abschreckungswirkung des PPS ist so abstrakt und wenig quantifizierbar, dass sie nur als ein zusätzlicher Nutzen der umgesetzten PPS Maßnahmen anzusehen ist (Morral & Jackson 2009, S.24). Die Konzeption eines PPS orientiert sich an einem Neutralisieren eines Angriffs. Für dieses Neutralisieren müssen die Funktionen so ausgelegt sein, dass die Detektionsfunktion die verschiedenen Bedrohungen zuverlässig identifiziert, die Verzögerungsfunktion sie ausreichend verzögert und die Reaktionsfunktion sie erfolgreich neutralisiert.

3. Risiko-Assessment

3.1. Identifikation von Risiken

Bedrohungsszenarien

Die Aufgabe der Risikoidentifikation ist das systematische, konsistente und vollständige Erfassen aller in dem Untersuchungszusammenhang relevanten bereits existierenden, bzw. in der Zukunft möglicherweise bestehenden Risiken sowie ihrer Ursachen für ein Objekt oder eine Gruppe von Objekten. Die Identifikation muss dementsprechend sowohl gegenwarts- als auch zukunftsbezogen sein. Eine Zusammenstellung von möglichen Bedrohungsszenarien ist Voraussetzung für die sich daran anschließende Bestimmung der Risikoelemente unter diesen Szenarien. Nur wenn bestehende Bedrohungen identifiziert und beschrieben sind, kann im nächsten Schritt ein Messen und Analysieren der Bedrohungen stattfinden.

Systematisierung und Abgrenzung von Risiken

Entscheidend für die Systematisierung und Abgrenzung von Risiken und Objekten ist die dem Untersuchungszusammenhang zugrundeliegende Fragestellung (Wolke 2009, S.6). Hieraus erschließt sich zum einen, welche Risikoarten zu betrachten sind und zum anderen, für welche Objekte die Risiken systematisiert werden müssen. In diesem Untersuchungszusammenhang ist sowohl die Art des Risikos - anthropogene[11] Piraterie- und Terrorismus-Risiken - als auch das zu untersuchende Objekt - Schiff - durch die Fragestellung vorgegeben.

Dimensionen zur Unterscheidung von Risiken

Eine Unterscheidung verschiedener Risiken innerhalb einer Risikoart findet sinnvollerweise anhand ihrer Natur, ihrem Ursprung, der zeitlichen Dimensionen, dem Umfang ihrer Auswirkungen sowie der betroffenen Verantwortungsbereiche statt (Rosenkranz & Missler-Behr 2005, S.145). Für anthropogene Risiken ist es darüber hinaus zweckmäßig, den Angreifer anhand von Dimensionen wie Typ, Motivation, Organisationsgrad und Grad der Gewaltanwendung bzw. Gewaltbereitschaft zu charakterisieren (Moteff 2005, S.7). Hinsichtlich des Ursprungs ist zwischen einer Bedrohung, die innerhalb - durch einen sogenannten Innentäter - oder außerhalb - durch einen Außentäter - des bedrohten Objekts entsteht, zu unterscheiden. Ein Innentäter ist berechtigt auf eine Organisation mit ihren Systemen, Informationen und Ressourcen zuzugreifen.[12] Eine interne Bedrohung ist das Risiko, das darin besteht, dass ein Innentäter seinen Zugriff nutzt, um der Organisation einen Schaden zuzufügen (Blackwell 2009, S.9). Entsprechend beginnt ein Außentäter, der nicht berechtig ist auf die Organisation zuzugreifen, einen Angriff von außerhalb des Objektes.

Methodiken der Risikoidentifikation

Grundsätzlich kann die Identifikation von Risiken entweder über eine Ableitung aus Erfahrungs- oder Vergangenheitswerten, über eine Antizipation möglicher zukünftiger Risiken sowie eine Kombination beider Vorgehensweisen stattfinden (Rosenkranz & Missler-Behr 2005, S.146). McGill (2008, S.15–16) unterscheidet darüber hinaus zwischen einem bedrohungsorientierten und einem objektorientierten Vorgehen bei der Identifikation von Risiken.

Vergangenheitsbezogene Identifikation

Die vergangenheitsbezogene Identifikation greift auf verfügbare Dokumente, Aufzeichnungen oder interne bzw. externe Statistiken zu, um darin Risiken zu identifizieren, die in der Vergangenheit aufgetreten sind. Diese werden anschließend dahingehend analysiert, ob sie auch für die Gegenwart bzw. Zukunft im betrachteten Untersuchungszusammenhang relevant sind, und, wenn dies der Fall ist, in die Untersuchung übernommen (Rosenkranz & Missler-Behr 2005, S.146).

Antizipative Identifikation

Die Antizipation möglicher Risiken ist insbesondere bei der Betrachtung noch nicht dagewesener Zusammenhänge und Prozesse unverzichtbar. Bei dieser Vorgehensweise ist es möglich, strukturell neue Risiken zu identifizieren, die nicht auf der Basis von Vergangenheitsdaten klassifizier- und bewertbar sind. Für die antizipative Risiko-

11 anthropogen: durch den Menschen beeinflusst, verursacht (Duden 2007).

12 Ein Innentäter kann weiter unterschieden werden in einen tatsächlich berechtigten, autorisierten und einen sich als berechtigt ausgebenden, unautorisierten Innentäter. Der autorisierte Innentäter kann nur detektiert werden, indem seine Intention, einen Schaden herbeizuführen, entdeckt wird oder er bei der Schaden herbeiführenden Handlung selber erkannt wird. Der unautorisierte Innentäter kann darüber hinaus auch dadurch detektiert werden, dass seine Tarnung als ein Fehlen der Berechtigung aufgedeckt wird.

identifikation bieten sich verschiedene Kreativitätstechniken, Szenarioanalysen oder Simulationsmodelle an (Rosenkranz & Missler-Behr 2005, S.147–148).

Bedrohungsorientierte Identifikation

Die bedrohungsorientierte Identifikation beginnt bei Überlegungen zu den Fähigkeiten und Intentionen möglicher Angreifer, welche sie aus historischen Ereignissen und / oder (Geheimdienst-) Einschätzungen ableitet. Ausgehend hiervon findet eine Identifikation von Szenarien statt, die unter den angenommenen Fähigkeiten möglich sind, unter den angenommenen Intentionen für den Angreifer wünschenswert erscheinen sowie eine Bedrohung für das betrachtete Objekt darstellen. Bedrohungsorientierte Vorgehensweisen eignen sich gut, um wohlbekannte Risiken, deren Eintreten zuverlässig anhand von Vergangenheitsdaten ableitbar ist, zu identifizieren. Sie sind allerdings weniger geeignet, innovative, vorher nicht dagewesene Bedrohungen zu erkennen (McGill 2008, S.16).

Objektorientierte Identifikation

Der objektorientierte Ansatz geht in entgegengesetzter Richtung vor. Hier findet zunächst eine Analyse des risikoexponierten Objektes statt. Ziel ist es, alle für die einzelnen Elemente des Objekts insgesamt denkbaren Bedrohungen zusammenzutragen und eine Abschätzung zu den damit verbundenen Auswirkungen zu treffen. Aufbauend darauf können Bereiche als Element-Bedrohungs-Kombinationen ermittelt werden, die mit erheblichen Auswirkungen verbunden sind und damit als kritisch angesehen werden. Diese sensiblen Bereiche des Objektes gilt es vor einem Angriff zu schützen (Lave 2002, S.1). Anschließend folgt basierend auf Überlegungen zu Intention und Fähigkeit möglicher Angreifer eine Abschätzung über die Höhe der tatsächlichen Bedrohung für alle oder nur die als sensibel identifizierten Bereiche ausfällt. Ein Vorteil des objektorientierten Vorgehens ist die geringere Unsicherheit, da nicht von Vermutungen über Fähigkeiten und Intentionen möglicher Angreifer ausgegangen, sondern an den verlässlichen Informationen über das bedrohte Objekt angesetzt wird. Außerdem ist die Gefahr eine Bedrohung zu übersehen, bei der Suche nach allen denkbaren Bedrohungen, verglichen mit einer Suche nach unter bestimmten angenommenen Fähigkeiten und Intentionen möglichen Bedrohungen, geringer (McGill 2008, S.16).

Bedrohungsszenarien finden sich in der Literatur. Sie dienen als Grundlage für die Untersuchung der Vulnerabilität

In der Literatur findet sich eine Vielzahl von Bedrohungsszenarien, die im Zusammenhang mit Piraterie und maritimem Terrorismus identifiziert sind. Zu Bedrohungen durch Piraterie sei unter anderem verwiesen auf Johnson & Valencia (2005); Ong-Webb (2006); Chalk (2008); Mischuk (2009); Flottenkommando Marine (2010); UNODC (2010); Petretto (2011). Bedrohungen, die im Zusammenhang mit maritimem Terrorismus bestehen, finden sich unter anderem bei Gunaratna (2003); Stehr (2004); Ong-Webb (2006); Greenberg u. a. (2006); Jenisch (2010). In dieser Untersuchung wird keine eigenständige Identifikation vorgenommen. Da jedoch Risikomessung und Risikoanalyse auf den Ergebnissen der Risikoidentifikation aufbauen, bezieht sich die Ausarbeitung auf bereits identifizierte Bedrohungsszenarien. Die Auswahl der Bedrohungsszenarien, die genauer betrachtet werden, ist in Kapitel 4.1 dargestellt.

3.2. Bestimmung des Risikoelements Gefährdung

Gefährdung besteht nur bei Intention und Fähigkeit

Von Personen, Personengruppen oder Organisationen geht nur dann eine Gefährdung aus, wenn bei diesen sowohl die Intention als auch die Fähigkeit vorhanden ist, die zur Bedrohung führende Handlung durchzuführen. Weder eine Intention ohne die entsprechenden Fähigkeiten noch die nötigen Fähigkeiten ohne eine Intention führen zu einer Gefährdung und damit potentiell zu einem Risiko (Willis u. a. 2005, S.6). Dementsprechend ist es bei der Messung des Risikos angebracht, sowohl die Intention als auch die Fähigkeit als Determinanten der Gefährdung zu betrachten.

Schwierigkeiten bezüglich der Bestimmung von Intention und Fähigkeit

Im Gegensatz zu vielen anderen Risiken sind anthropogene Bedrohungen der Sicherheit eines Objekts durch vorsätzlich, innovativ und unberechenbar handelnde Angreifer charakterisiert. Diese wählen beeinflusst durch ihr Ziel, ihre Motivation und ihre Ressourcen aus einer Vielzahl verschiedener Angriffsziele und innovativer Angriffsvorgehensweisen entsprechend der erwarteten Erfolgsaussichten, Risiken und Auswirkungen eine Variante aus (McGill u. a. 2007, S.1265–1266). Aus Zielen und Motivation lässt sich die Intention ableiten. Die Ressourcen bestimmen maßgeblich die Fähigkeiten. Die Informationsbeschaffung zu beiden Faktoren greift auf zugängliche (Geheimdienst-) Informationen, historische Analysen und Expertenmeinungen zurück (Willis u. a. 2005, S.14). Experten sind sich jedoch oftmals hinsichtlich der genauen Ziele und Ressourcen bestimmter (terroristischer) Gruppierungen uneinig. Zu anderen Gruppierungen existieren unter Umständen keine Informationen oder ihre Existenz ist gänzlich unbekannt. Dementsprechend vage sind Beurteilungen zu Intention und Fähigkeiten potentieller Angreifer. Folglich ist die Einschätzung der Gefährdung anfällig gegenüber einer signifikanten Über- oder Unterschätzung. Bei der Bestimmung von Wahrscheinlichkeiten eines Angriffes wirkt sich zusätzlich erschwerend aus, dass Angreifer unter Umständen adaptiv auf getroffene Schutzmaßnahmen reagieren, indem sie Angriffsvorgehensweisen, Angriffsziele oder Angriffszeitpunkte verändern (Murray-Tuite & Fei 2010, S.397).

Hohe Unsicherheit bezüglich der Gefährdung

Die Gefährdung ist folglich ein mit hoher Unsicherheit versehenes Risikoelement (Ayyub u. a. 2007, S.790) und sollte nur als grobes Maß der Wahrscheinlichkeit eines Angriffs aufgefasst werden (Willis u. a. 2005, S.14).

Risikoveränderung über das Risikoelement Gefährdung

Intention und Fähigkeit eines Angreifers sind nicht nur mit einer hohen Unsicherheit verbunden, sondern für den Angegriffenen nicht, oder nur sehr begrenzt, direkt beeinflussbar (Ferriere u. a. 2005, S.5).

Bestimmung der Fähigkeit

Einige Terrorismusszenarien, wie Selbstmordattentate mit konventionellem Sprengstoff, stellen vergleichsweise geringe Anforderungen an die Fähigkeiten eines Angreifers. Demgegenüber sind andere Szenarien, wie etwa Angriffe mit chemischen, biologischen, radiologischen oder nuklearen Waffen, nur mit speziellem Expertenwissen durchführbar (Greenberg u. a. 2006, S.146). Diese mit verschiedenen Bedrohungsszenarien verbundenen Anforderungen an die Fähigkeiten eines potentiellen Angreifers gilt es zu ermitteln. Dabei sind neben direkten auch indirekte Fähigkeiten (wie z. B. das Vermögen, ein Team zu organisieren oder die Verbindungen, um bestimmte Käufe auf dem Schwarzmarkt zu tätigen) zu berücksichtigen (RAMCAP 2006, S.42). Von Szenarien, die höhere Ansprüche an die Fähigkeiten stellen, wird ausgegangen, dass sie insgesamt weniger wahrscheinlich sind. Um als Maß in die Gefährdung einzugehen, müssen die Anforderungen an die Fähigkeiten noch mit den tatsächlich

vorhandenen Fähigkeiten der potentiellen Angreifer verglichen werden. Hierbei sind nicht nur die gegenwärtigen sondern auch zukünftig zu erwartende Fähigkeiten zu berücksichtigen. Bei fehlenden Informationen über die vorhandenen Fähigkeiten kann der Level der Anforderungen als Maß in die Bestimmung der Gefährdung einfließen.

Beispiel einer qualitativen Skala zur Bewertung der Fähigkeiten

Ein Beispiel einer qualitativen Skala, mit der Greenberg u.a. (2006, S.147) die benötigten Fähigkeiten unter verschiedenen Bedrohungsszenarien ermittelt, ist in Tabelle 1 dargestellt.

Tabelle 1: Beispiel einer Skala zur qualitativen Bestimmung der Fähigkeiten, welche für die Durchführung eines Bedrohungsszenarios vorausgesetzt werden

BEWERTUNG	DETERMINANTEN FÜR DIE BEWERTUNG DER ERFORDERLICHEN FÄHIGKEITEN
1 (hoch)	Hochspezialisierte Fähigkeiten: setzt hochspezialisierte sowie seltene Fähigkeiten wie die Beherrschung nuklearer Anlagen, industrielle Produktion, Umgang mit Präzisions- und Produktionstechnologien im Geheimen voraus.
2	Spezialisierte Fähigkeiten: setzt spezielle Fähigkeiten, wie das Hacken von Computern, die Steuerung von Fahr- / Flugzeugen oder die Planung und Implementierung komplexer Operationen voraus.
3	Militärisches Expertenwissen: Umgang mit verschiedenen Sprengstoffen, Einsatz von komplizierten Waffensystemen.
4	Militärisches Grundlagenwissen: Militärisches Training inklusive Kampftraining, Umgang mit Waffen sowie Nahkampffähigkeiten.
5 (gering)	Grundfertigkeiten: keine besonderen Vorrausetzungen, kann mit einfacher Schulbildung umgesetzt werden.

Quelle: Greenberg u.a. (2006, S.147). *Eigene Übersetzung.*

Bestimmung der Intention

Die Intention ist ein Maß dafür wie sehr ein Bedrohungsszenario zu einer Erfüllung der Ziele eines potentiellen Angreifers beiträgt. Um zu ermitteln, ob und in welchem Umfang ein Bedrohungsszenario den Intentionen potentieller Angreifer entspricht bzw. diese erfüllt, sind Erfolgsaussichten, Risiken und Auswirkungen der Bedrohungsszenarien mit Motivationen und Zielen der Angreifer zu vergleichen. Dabei ist zu berücksichtigen, dass sich die Ziele und Motivationen verschiedener potentieller Angreifer voneinander unterscheiden und folglich unterschiedliche Aspekte bei der Konstruktion einer Skala zur Messung der Intention berücksichtigt werden müssen. Im Unterschied zu Piraten für die der Umfang potentieller Beute eine entscheidende Rolle hinsichtlich der Intention spielt, ist dieser Aspekt beispielsweise für Terroristen von keiner, oder einer nachrangigen, Bedeutung. Hier stehen Aspekte wie etwa das Schadenspotential oder ein Erzeugen medialer Präsenz im Vordergrund. Entsprechend ist es notwendig, für verschiedene, hinsichtlich ihren Zielen und Motivationen homogenen Gruppen von Angreifern jeweils entsprechend ausgelegte Skalen zu entwickeln.

Beispiel einer qualitativen Skala zur Bewertung der Intention

Ein Beispiel für eine, entsprechend den Zielen und Motivationen islamistischer Terroristen angepasste, Skala zur qualitativen Ermittlung der Intention ist in Tabelle 2 dargestellt. Die in diesem Zusammenhang relevanten Aspekte sind: Anzahl an Toten und Verletzten, Ausmaß des ökonomischen Schadens, Umfang der zu erwartenden Medi-

enberichterstattung und symbolische Bedeutung des Angriffszieles bzw. -ortes (Greenberg u. a. 2006, S.145–146).

Tabelle 2: Beispiel einer Skala zur qualitativen Bestimmung der Intention, die mit der Durchführung eines Bedrohungsszenarios verbunden wird

BEWERTUNG	DETERMINANTEN FÜR DIE BEWERTUNG DER INTENTION
1 (gering)	Folgen der Handlung würden im Widerspruch stehen zu den Zielen der Terroristen.
2	Menschliche Opfer, aber ohne Medienwirksamkeit, symbolische Bedeutung oder ökonomische Konsequenzen.
3	Menschliche Opfer und ökonomische Konsequenzen, aber ohne symbolische Bedeutung oder Medienwirksamkeit.
4	Menschliche Opfer, ökonomische Konsequenzen und Medienwirksamkeit, aber ohne symbolische Bedeutung.
5 (hoch)	Signifikante Anzahl menschlicher Opfer, erhebliche symbolische Bedeutung, umfangreiche Medienwirksamkeit und ökonomische Konsequenzen.

Quelle: Greenberg u.a. (2006, S.146) . *Eigene Übersetzung.*

3.3. Bestimmung des Risikoelements Vulnerabilität

Vulnerabilität

Die Vulnerabilität beschreibt die Verwundbarkeit, welche ein angegriffenes Objekt unter einem Bedrohungsszenario aufweist. Sie kann als ein Maß aufgefasst werden, das angibt wie groß die Wahrscheinlichkeit ist, dass ein Angreifer mit einem Angriff Erfolg hat (RAMCAP 2006, S.34).

Vulnerabilität ist das am genauesten bestimmbare Risikoelement

Die Vulnerabilität ist das am genauesten bestimmbare und folglich mit der geringsten Unsicherheit behaftete Risikoelement. Grund hierfür ist, dass die Vulnerabilität durch die Charakteristika des angegriffen Objekts determiniert ist, dessen Ausprägungen bekannt sind (Ayyub u. a. 2007, S.790).

Faktoren und Aspekte, welche die Vulnerabilität beeinflussen

Genauso wie die Risikoelemente Gefährdung und Auswirkungen wird die Vulnerabilität durch verschiedene Faktoren und Aspekte charakterisiert. Zu berücksichtigen sind physische, technische, operative und organisatorische Aspekte (Moteff 2005, S.8; Roper 1999, S.65). Für die Vulnerabilität eines Schiffes sind Konstruktion (z.B. Design des Schiffsrumpfes), technische Ausstattung (z.B. Radar) und operativer Betrieb (z.B. Überwachung des Schiffsumfeldes, Zugangskontrollen zum Schiff oder Inspektionen der Schiffsladung) ausschlaggebend (Greenberg u. a. 2006, S.147).

Gegenmaßnahmen beeinflussen die Vulnerabilität

Im Zusammenhang mit der Vulnerabilität eines Objektes spielen darüber hinaus Gegenmaßnahmen, deren Zweck eine Reduktion der Vulnerabilität ist, eine Rolle. Bei einem Schiff setzen sie an den Aspekten Konstruktion bzw. technische Ausstattung (als technische Gegenmaßnahmen) und operativer Betrieb (als operative Gegenmaßnahmen) an. Eine exakte Zuordnung der Maßnahmen ist dabei jedoch oft nicht möglich, da technische Maßnahmen in vielen Fällen durch eine operative Umsetzung in ihrer Effektivität bedingt sind und operative Maßnahmen sich vielfach technischer

Hilfsmittel bedienen.[13] Auch eine Trennung von Vulnerabilität, die durch das Schiff gegeben ist und Vulnerabilität, die durch Gegenmaßnahmen beeinflusst wurde, ist problematisch. Zum einen können bereits Gegenmaßnahmen an einem Schiff bestehen, wenn die Vulnerabilität ermittelt wird, so dass es wenig praktikabel ist, diese bei der Analyse des Schiffes zu exkludieren. Zum anderen können bestimmte Einrichtungen des Schiffes, deren primärer Zweck nicht die Verringerung der Vulnerabilität ist, dennoch bei entsprechendem Einsatz zu einer Verringerung beitragen. Folglich ist es sinnvoll, die Vulnerabilität des Schiffes und die Einflüsse, welche die Gegenmaßnahmen auf diese haben, unter derselben Methodik in einem Schritt zu betrachten.

Gegenmaßnahmen als weiterer Einflussfaktor in der Risikofunktion

Gegenmaßnahmen können als ein weiterer Einflussfaktor in die Risikofunktion integriert werden, wie in Formel 3 dargestellt. Allerdings ist hier der Zusammenhang zwischen Gegenmaßnahmen und Risiko umgekehrt: je mehr Gegenmaßnahmen vorhanden sind desto geringer wird das Risiko.

Formel 3: Risiko als Funktion der Risikoelemente und Gegenmaßnahmen

$$\text{Risiko (Gefährdung, Vulnerabilität, Auswikung, Gegenmaßnahmen)}$$

Risikoveränderung über das Risikoelement Vulnerabilität

Somit besteht bei der Vulnerabilität, im Gegensatz zu den anderen Risikoelementen, ein Ansatzpunkt, an dem Betroffene direkt Einfluss auf das bestehende Risiko nehmen können (Ferriere u. a. 2005, S.6). Das Vermögen, die Vulnerabilität eines Objektes oder Systems zu bestimmen, ist damit nicht nur eine Voraussetzung um das Risiko, das von einer Bedrohung ausgeht, abzuschätzen, sondern auch um zu ermitteln, welche Gegenmaßnahmen einzusetzen sind, sodass die Vulnerabilität und damit auch das Risiko verringert werden.

Vulnerabilitäts-Assessment

Typischerweise wird zur Bestimmung der Vulnerabilität ein Vulnerabilitäts-Assessment als eine systematische Evaluation unter Anwendung qualitativer oder quantitativer Methoden durchgeführt. Ziel ist die Ermittlung der Widerstandsfähigkeit eines Objektes gegenüber einer bestimmten Bedrohung (Garcia 2006, S.1). Dabei kann die Vielzahl relevanter Eigenschaften des Systems mit etwaigen Abhängigkeiten der Eigenschaften untereinander sowie Abhängigkeiten zu verschiedenen Faktoren außerhalb des betrachteten Objektes zu einer hohen Komplexität des abstrakten Konzeptes der Vulnerabilität führen. Liegt eine hohe Komplexität vor, ist bei der Bestimmung der Vulnerabilität eine Vereinfachung der Zusammenhänge vorzunehmen ohne das Wesentliche des zu messenden Phänomens zu verlieren (Lenz 2009, S.47). Nur wenn die damit verbundenen Verluste an Genauigkeit in Kauf genommen werden, ist eine praktikable Abschätzung der Vulnerabilität möglich.

Darstellung der Vulnerabilität mithilfe eines Indikators

Eine direkte Messung der Vulnerabilität als abstraktes Phänomen ist nicht möglich (Lenz 2009, S.47). Als geeignetes Hilfsmittel finden hier Vulnerabilitätsindikatoren, welche die verschiedenen Dimensionen der Vulnerabilität abbilden, Anwendung. In der Literatur finden sich unterschiedliche Methoden zur Entwicklung von Vulnerabilitätsindikatoren, die sich größtenteils auf die Vulnerabilität sozialer Gruppen, Gesell-

[13] Technische Maßnahmen, wie etwa ein (leistungsfähigeres) Radar, werden in ihrer Auswirkung auf die Vulnerabilität entscheidend davon beeinflusst, wie das Radar operativ eingebunden wird. Operative Maßnahmen, z.B. bessere Überwachung des Schiffsumfeldes, bedienen sich technischer Hilfsmittel wie Radar oder Fernglas.

schaften oder Nationen, jedoch nicht auf die physische Vulnerabilität eines Objektes Schiff, beziehen und nur bedingt übertragbar sind (Lenz 2009, S.48). Dementsprechend muss ein passender Ansatz gefunden werden, aus dem sich geeignete Einzelindikatoren zur Beschreibung der Vulnerabilität des Objektes Schiff ableiten lassen.

PPS als Ansatz um Vulnerabilität in einem Indikator abzubilden

Ein vielfach angewandtes Konzept, nach dem Maßnahmen zur Verringerung der Vulnerabilität eines Objektes ausgelegt werden, ist das in Kapitel 2.3 beschriebene PPS. Hierbei müssen die ergriffenen Maßnahmen zur Abwehr eines Angriffes die Funktionen Detektion, Verzögerung und Reaktion erfüllen (RAMCAP 2006, S.55). Dieser Ansatz wird übernommen, um die Vulnerabilität eines Schiffes (unter Berücksichtigung etwaiger Gegenmaßnahmen) in einem Indikator abzubilden. Das Konzept für die Entwicklung des Vulnerabilitätsindikators ist in Kapitel 4 dargestellt.

3.4. Bestimmung des Risikoelements Auswirkungen

Dimensionen zur Messung der Auswirkungen

In den Auswirkungen wird versucht zu erfassen, wie die zu erwartenden Folgen verschiedener Bedrohungsszenarien aussehen. Dazu sind geeignete Dimensionen festzulegen, anhand derer das Ausmaß der Folgen gemessen wird (Pate-Cornell & Guikema 2002, S.3). Mögliche Dimensionen sind (RAMCAP 2006, S.29; Moteff 2005, S.5; Ehrhart u. a. 2011, S.71):

- Aspekte der menschlichen Sicherheit und Gesundheit
- Ökonomische Verluste und Effekte
- Auswirkungen auf die Umwelt
- Auswirkungen auf die Soziokultur der Gesellschaft
- Auswirkungen auf die nationale Sicherheit
- Verlust materieller und immaterieller Güter
- Nachteilige Effekte auf Markenimages und -werte
- Auswirkungen auf die öffentliche Meinung / das öffentliche Vertrauen
- Psychologische Auswirkungen

Messbarkeit der Dimensionen

Bei der Auswahl geeigneter Dimensionen spielt deren Messbarkeit eine entscheidende Rolle. Vergleichsweise einfach ist die Messung bei Dimensionen, die sich quantitativ darstellen lassen (etwa die Anzahl von Verletzten oder Toten oder der ökonomische Schaden als Geldeinheit). Wesentlich problematischer ist die Abschätzung für „weiche“ Faktoren wie psychologische Auswirkungen oder Auswirkungen auf die öffentliche Meinung. Sie lassen sich nicht quantitativ ermitteln und sind dementsprechend nur anhand von subjektiv festgelegten qualitativen Skalen ermittelbar (McGill 2008, S.20).

Zusammenführen der Dimensionen

Bei Messung der Auswirkungen anhand mehrerer Dimensionen stellt sich die Frage ob, und wenn ja wie diese zu einem Wert durch Überführung in dieselbe Einheit kombinierbar und vergleichbar sind. Um etwa Aspekte der menschlichen Sicherheit und Gesundheit in monetären Einheiten darzustellen, kann, wenn es als ethisch vertretbar angesehen wird, auf Ansätze wie den „Wert eines statistischen Lebens“ (value of statistical life) zurückgegriffen werden (Viscusi & Aldy 2003, S.5).

Sekundäre Effekte

Neben direkten Auswirkungen gilt es auch sekundäre Effekte zu betrachten (Pate-Cornell & Guikema 2002, S.3). Sekundäre Effekte sind Folgen der direkten und kön-

nen diese um ein Vielfaches übertreffen (Crist 2003, S.23). Beispiele sekundärer Effekte sind etwa die Auswirkungen von Unterbrechungen des Telekommunikationsnetzes auf das Bankensystem oder Auswirkungen von Unterbrechungen der Stromversorgung auf das produzierende Gewerbe (Pate-Cornell & Guikema 2002, S.3)

Risikoveränderung über das Risikoelement Auswirkungen

Prinzipiell ist es möglich durch Einflussnahme auf die Auswirkungen einer Bedrohung das Risiko eines Objektes zu beeinflussen. Dazu müssen die Eigenschaften des Objektes dahingehend verändert werden, dass sich die Auswirkungen unter den Bedrohungsszenarien verringern (Ferriere u. a. 2005, S.5–6). Dies ist jedoch nur sinnvoll, solange sich durch eine Veränderung der Eigenschaften der Gebrauchsnutzen des Objektes nicht ändert. Bei einem Tankschiff, das kein Öl geladen hat, sind beispielsweise die mit einem Angriff verbundenen Auswirkungen deutlich geringer, der Gebrauchsnutzen des Schiffes ist jedoch nicht mehr gegeben.

Beispiel qualitativer Skalen zur Bewertung der Auswirkungen

Ein Beispiel der qualitativen Messung von Auswirkungen verschiedener terroristischer Bedrohungsszenarien anhand von Skalen ist in Tabelle 3 und Tabelle 4 dargestellt (Greenberg u. a. 2006, S.150–152). Hier werden die Dimensionen der menschlichen Sicherheit und Gesundheit - gemessen an der Anzahl der getöteten und verletzten Menschen - sowie ökonomische Verluste und Effekte - gemessen am ökonomischen Schaden - einzeln berücksichtigt und nicht kombiniert.

Tabelle 3: Beispiel einer Skala zur qualitativen Bestimmung von Auswirkungen anhand der Dimension Auswirkungen auf die menschliche Gesundheit

BEWERTUNG	DETERMINANTEN FÜR DIE BEWERTUNG DER AUSWIRKUNGEN AUF DIE MENSCHLICHE GESUNDHEIT
1 (gering)	Weniger als 10 Tote oder Verletzte.
2	10 - 100 Tote oder Verletzte.
3	100 – 1,000 Tote oder Verletzte.
4	1,000 – 10,000 Tote oder Verletzte.
5 (hoch)	Mehr als 10,000 Tote oder Verletzte.

Quelle: Greenberg u.a. (2006, S.151). *Eigene Übersetzung.*

Tabelle 4: Beispiel einer Skala zur qualitativen Bestimmung von Auswirkungen anhand der Dimension ökonomische Verluste und Effekte

BEWERTUNG	DETERMINANTEN FÜR DIE BEWERTUNG DER ÖKONOMISCHEN VERLUSTE UND EFFEKTE
1 (gering)	Mehrere zehn Millionen $ ökonomischer Schaden.
2	Hunderte von Millionen $ ökonomischer Schaden.
3	Mehrere Milliarden $ ökonomischer Schaden.
4	Mehrere zehn Milliarden $ ökonomischer Schaden.
5 (hoch)	Hunderte von Milliarden $ ökonomischer Schaden.

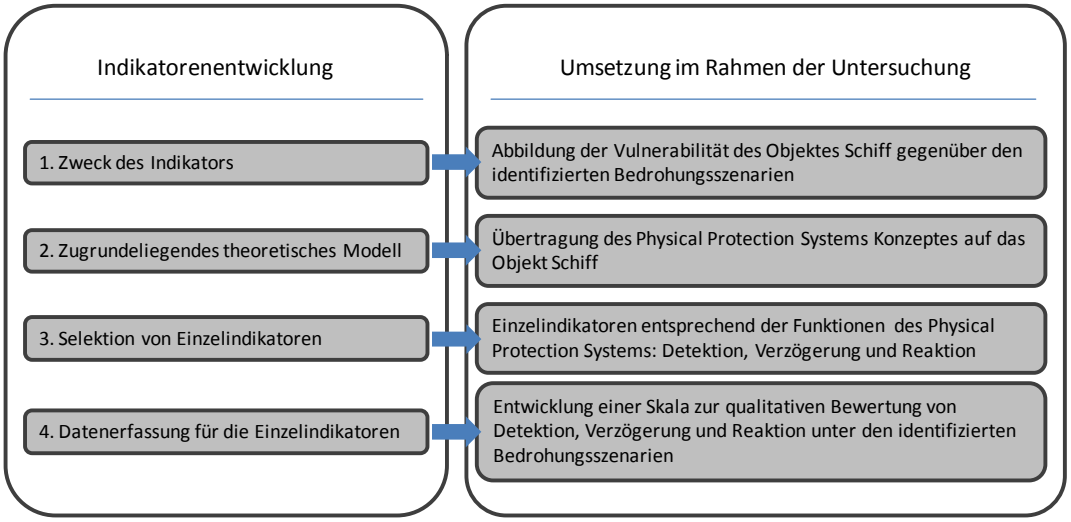
Quelle: Greenberg u.a. (2006, S.152). *Eigene Übersetzung.*

4. Konzept eines qualitativen Vulnerabilitätsindikators

Konzeptionelle Grundlagen der Entwicklung des Vulnerabilitätsindikators

Der im Folgenden entwickelte Ansatz zur Bewertung der Vulnerabilität eines Schiffes mithilfe eines Indikators folgt dem Prozess der Indikatorenentwicklung aus Kapitel 2.2.3. In Kapitel 2.1.3 wurde darauf eingegangen, dass die Messung von Risikoelementen anhand von qualitativen oder quantitativen Methoden vorgenommen werden kann. Der hier entwickelte Indikator ist qualitativer Natur. Dies ist begründet in einem geringeren Aufwand für die Erfassung der Ausprägung der Einzelindikatoren als bei einem quantitativen Vorgehen. Dadurch wird das Vorgehen der Forderung nach einem praktikablen Konzept gerecht. Der Indikator ist jedoch so konzipiert, dass die entwickelte Struktur als Grundlage für eine Erweiterung zu einem quantitativen Indikator dienen kann. Eine Aggregation der Einzelindikatoren zu einem zusammengefassten Indikator erfolgt nicht. Es wird sich in diesem ersten Ansatz darauf beschränkt die Einzelindikatoren schlüssig zu entwickeln. Die Umsetzung der einzelnen Schritte des Prozesses der Entwicklung des Vulnerabilitätsindikators, ist in Abb. 3 zusammengefasst und wird im Folgenden beschrieben. Die Schritte 5 und 6 der Indikatorenentwicklung werden nicht umgesetzt, da sie nur für einen aggregierten Indikator relevant sind. Die in Schritt 7 vorgesehene Sensitivitätsanalyse geht über den Rahmen dieser Arbeit hinaus und wird dementsprechend nicht betrachtet.

Abb. 3: Darstellung der Indikatorenentwicklung



4.1. Zweck des Indikators

Zweck ist die Vulnerabilität eines Schiffes abzubilden

Zweck des Indikators ist die Vulnerabilität eines Schiffes gegenüber Bedrohungsszenarien, die sich durch Piraterie und maritimen Terrorismus ergeben, abzubilden. Entsprechend ist das untersuchte Indikandum das Risikoelement Vulnerabilität. Der Indikator bildet ab, wie groß die Wahrscheinlichkeit ist, dass ein ausgeführter Angriff auf ein Schiff Erfolg hat. Dabei ist sowohl die dem Schiff innewohnende Vulnerabilität als auch eine Reduktion der Vulnerabilität, die sich aufgrund von an Bord befindlichen Gegenmaßnahmen ergibt, mit dem Indikator nachzuzeichnen.

4.2. Zugrundeliegendes theoretisches Modell

Konzept des PPS bildet zugrundeliegendes Modell für den Vulnerabilitätsindikator

Als konzeptionelles Modell, das der Auswahl von relevanten an die Fragestellung angepassten Einzelindikatoren zugrunde liegt, dient das Konzept des PPS. Die Aufgabe eines PPS ist es, ein Objekt gegenüber einem Angriff zu schützen. Es bestimmt damit entscheidend die Wahrscheinlichkeit, dass ein Angriff Erfolg hat. Das Ziel des Indikators besteht genau darin diese Wahrscheinlichkeit abzubilden. Somit stellt das Konzept des PPS ein geeignetes Modell für die Bestimmung der Vulnerabilität dar.

Funktionen des PPS bilden den Rahmen des Vulnerabilitätsindikators

Die Funktionen, die ein PPS erfüllen muss, sind: (1) eine Detektion des Angriffs, (2) ein Verzögern des Angriffs und (3) eine Reaktion auf den Angriff. Um zu bestimmen, wie groß die Wahrscheinlichkeit ist, eine Bedrohung abzuwehren, bietet es sich an, die Ausprägung dieser Funktionen an dem betrachteten Objekt zu untersuchen. Je besser die Funktionen erfüllt sind, desto wahrscheinlicher ist es, eine Bedrohung erfolgreich abzuwenden.

4.3. Selektion von Einzelindikatoren

Einzelindikatoren: Detektion, Verzögerung und Reaktion

Die Einzelindikatoren, die eine Darstellung der Vulnerabilität eines Schiffes gegenüber einer Bedrohung ermöglichen, entsprechen den Funktionen des PPS: (1) Detektion, (2) Verzögerung und (3) Reaktion. Es wäre auch denkbar diese Funktionen wiederum feiner zu untergliedern und durch entsprechende Einzelindikatoren auf einer niedrigeren Ebene abzubilden. Auch wenn so unter Umständen eine genauere Bestimmung der Vulnerabilität ermöglicht wird, soll im Hinblick auf die damit verbundene, abnehmende Praktikabilität darauf verzichtet werden. Bevor eine Bewertung der Ausprägung der Einzelindikatoren möglich ist, müssen die Funktionen des PPS an die Gegebenheiten, die im maritimen Umfeld eines Schiffes bestehen, angepasst werden.

4.3.1. Detektion

Detektion

Detektion ist das Erkennen einer potentiellen Bedrohung. Dieses findet meist innerhalb eines geschützten Bereichs um das gesicherte Objekt, oder an der Grenze des geschützten Bereichs statt. Je früher eine Bedrohung entdeckt wird, desto mehr Zeit steht für eine Reaktion zur Verfügung, weshalb es erstrebenswert ist, die Detektion bereits an der Grenze des geschützten Bereiches zu ermöglichen. Der geschützte Bereich weist mindestens einen regulären Zugang auf, über den autorisierte Personen und Gegenstände zu dem Objekt gelangen.

Detektion unterschiedlicher Bedrohungen

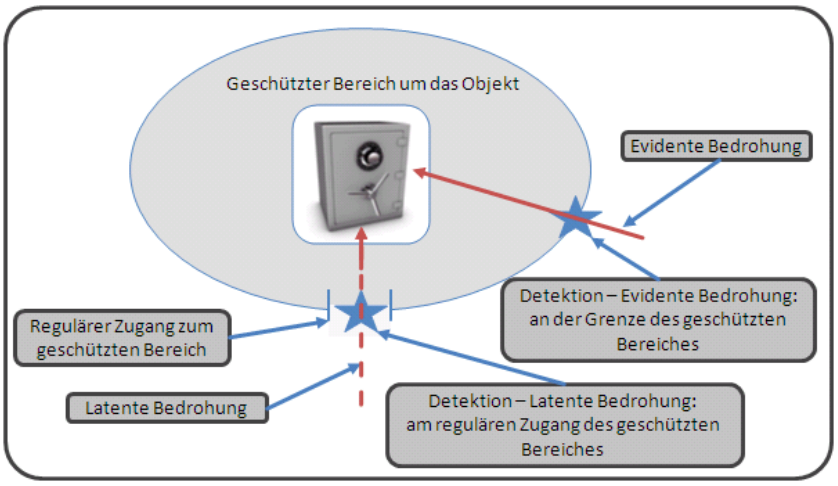
Bei der Untersuchung der Vulnerabilität ist es sinnvoll, die möglichen Bedrohungen anhand des Ursprunges sowie des Vorgehens des Angreifers zu charakterisieren. Entsprechend muss auch der Indikator für die Detektion an die betrachtete Bedrohung angepasst sein. Je nach Ursprung und Vorgehen sind verschiedene Aspekte ausschlaggebend, die bestimmen, ob eine Detektion der Bedrohung möglich und wie wahrscheinlich sie ist.

Ursprung einer Bedrohung

Für den Ursprung der Bedrohung wird zwischen einer latenten, im Inneren des Objektes zu Tage tretenden und einer evidenten, außerhalb des Objektes initialisierten, Bedrohung unterschieden. Eine Anpassung der Untersuchung der Vulnerabilität an das Vorgehen kann erst vorgenommen werden, wenn die zu untersuchenden Bedro-

hungsszenarien identifiziert und charakterisiert sind. Abb. 4 verdeutlicht die Unterschiede zwischen latenter und evidenter Bedrohung.

Abb. 4: Detektion für ein geschütztes Objekt – Latente und evidente Bedrohung



Latente Bedrohung

Bei einer **latenten**[14] **Bedrohung** gelangt 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 (etwa unter Zuhilfenahme eines gefälschten Ausweises / getarnt als eine reguläre Postsendung). Erst sobald sich Person oder Gegenstand innerhalb des geschützten Bereiches befinden, verliert sie / er den Deckmantel und nimmt die konkrete Form einer Bedrohung an. Die Detektion einer latenten Bedrohung findet am regulären Zugang statt. Unter die latente Bedrohung fällt auch eine Bedrohung durch einen Innentäter.

Evidente Bedrohung

Bei einer **evidente**[15] **Bedrohungen** ist – bei Identifikation dieser – unmittelbar klar, dass es sich um eine Bedrohung handelt. Darunter fällt ebenso ein unbemerktes verdecktes Vordringen durch den geschützten Bereich bis zum geschützten Objekt wie auch ein offenes Vorgehen unter Ausnutzung von Schnelligkeit oder durch Einsatz von Gewalt. Die evidente Bedrohung geht von einem Außentäter aus. Die Möglichkeit der Detektion einer evidenten Bedrohung muss entlang der gesamten Grenze des geschützten Bereiches vorgesehen sein, was auch den regulären Zugang beinhaltet. Es ist sinnvoll für die Detektion von evidenten Bedrohungen verschiedene an der Grenze des geschützten Bereiches angrenzende, in ihren Eigenschaften unterschiedliche Gebiete zu differenzieren. Befindet sich etwa auf der einen Seite des Objektes ein Waldgebiet und auf der anderen Seite das Meer, hat dieses einen Einfluss darauf, wie sich der Angreifer dem Objekt annähern kann. Dies bezieht sich sowohl darauf,

[14] Latent: versteckt, verborgen; [der Möglichkeit nach] vorhanden, aber [noch] nicht in Erscheinung tretend (Duden 2007).

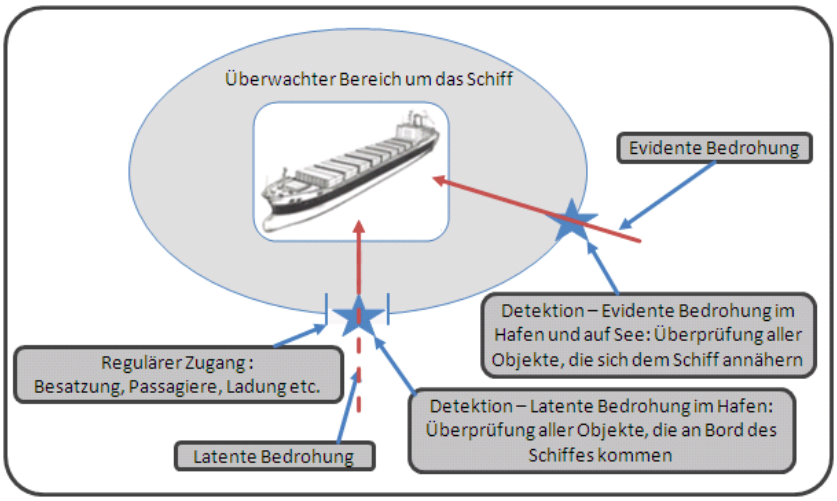
[15] Evident: offenkundig u. klar ersichtlich; offen zutage liegend (Duden 2007).

welche Vorgehensweisen denkbar sind, als auch, auf welche Weise eine Detektion möglich ist. [16]

Detektionsfunktion eines Schiffes

Für ein Schiff ist die Abgrenzung eines geschützten Bereiches problematisch. Es ist nicht möglich außerhalb des eigentlichen Schiffskörpers bauliche Maßnahmen (etwa Zäune) zu errichten, um einen Bereich abzugrenzen. Denkbar ist es, den geschützten Bereich auf den Schiffskörper selber zu beschränken und hier 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, etwa bei einem Angriff mit dem Ziel eine Bombe am Schiffskörper zur Explosion zu bringen, besteht keine Möglichkeit einer Verzögerung oder Reaktion. Dementsprechend ist es zweckmäßig die Detektion auf das Umfeld des Schiffes auszuweiten. Es findet eine Erfassung und Verfolgung aller sich dem Schiff nähernden Objekte, die sich innerhalb der Reichweite der Überwachung des Schiffsumfeldes befinden, statt. Kann ein auffälliges Objekt im Sinn einer potentiellen evidenten Bedrohung identifiziert werden, wird es bereits in größtmöglicher Entfernung des Schiffes auf seine Bedrohung hin evaluiert. So ist sichergestellt, eine Bedrohung so früh wie möglich zu erkennen. Abb. 5 stellt die latente und die evidente Bedrohung für ein Schiff dar.

Abb. 5: Detektion bei einem Schiff – Latente und evidente Bedrohung



Detektion einer latenten Bedrohung für ein Schiff

Eine latente Bedrohung nutzt den regulären Zugang zum Schiff. Dieser ist auf den Aufenthalt des Schiffes im Hafen beschränkt, wo Güter und Personen an Bord gelangen. [17] Die Detektion einer latenten Bedrohung für ein Schiff gestaltet sich folgendermaßen: Überprüfung aller Objekte (Ladung, Personen, Material), die an Bord des Schiffes kommen, dahingehend ob von ihnen potentielle Bedrohungen ausgehen. Bei

[16] Beispielsweise ist eine Annäherung durch den Wald mit einem Fahrzeug kaum zu erwarten. Eine visuelle Detektion eines Angreifers im Wald ist erschwert, da dieser von Bewuchs verdeckt wird. Eine Annäherung über das Meer ist sowohl über als auch unter Wasser möglich. Eine visuelle Detektion über Wasser ist schon in großer Entfernung möglich – unter Wasser jedoch erst bei Verlassen des Wassers.

[17] In Ausnahmefällen kann es auch vorkommen, dass ein regulärer Zugang zum Schiff nicht auf den Aufenthalt im Hafen beschränkt ist. Diese Fälle, etwa das an Bord Kommen von Lotsen oder der Küstenwache, sind nicht zu vernachlässigen sollen als Sonderfälle aber nicht weiter untersucht werden.

Identifikation einer potentiellen Bedrohung ist auch das Assessment der Bedrohung Teil der Detektion. 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 berücksichtigen, ob die Identität bzw. Integrität der Objekte zwischen Überprüfung und dem an Bord Kommen sichergestellt ist.

Einzelindikator Detektion – Latente Bedrohung

Der **Einzelindikator Detektion – Latente Bedrohung** bildet ab, wie groß die Wahrscheinlichkeit ist, ein Objekt, von dem eine Bedrohung ausgeht, zu identifizieren bevor / wenn es an Bord des Schiffes gelangt.

Detektion einer evidenten Bedrohung für ein Schiff

Die Detektion einer evidenten Bedrohung für ein Schiff gestaltet sich folgendermaßen: (1) Überwachung des Umfeldes des Schiffes und Identifikation potentieller Angreifer / eines potentiellen Angriffes. (2) Assessment und Entscheidung, ob es sich tatsächlich um einen Angreifer / Angriff handelt. Dabei gilt je größer die Entfernung, in der zuverlässig eine Detektion eines Angreifers / Angriffes möglich ist, desto besser, da somit die verfügbare Zeit zur Umsetzung von Verzögerung und Reaktion größer ist.

Einzelindikator Detektion – Evidente Bedrohung

Der **Einzelindikator Detektion – Evidente Bedrohung** bildet ab, wie groß die Wahrscheinlichkeit ist, einen Angreifer / Angriff in ausreichender Entfernung des Schiffes zu detektieren. Wie groß eine ausreichende Entfernung ist, hängt von dem Vorgehen des Angreifers und den an Bord befindlichen Verzögerungs- bzw. Reaktionsmaßnahmen ab.

Abschreckende Wirkung von Detektionsmaßnahmen

Die umgesetzten Detektionsmaßnahmen haben immer auch eine abschreckende Wirkung auf einen Angreifer oder können einen Angreifer zum Abbruch des Angriffs bewegen sobald er mit den tatsächlich vorhandenen Maßnahmen konfrontiert ist. Der Einzelindikator Detektion soll jedoch an der für ein Neutralisieren eines Angriffs nötigen Ausprägung der Detektionsfunktion gemessen werden. Damit wird bestimmt, was die Detektion leisten kann und nicht wie oder ob die Detektionsfunktion auf die Entscheidung eines potentiellen Angreifers wirkt.

4.3.2. Verzögerung

Verzögerung

Bestandteile der Verzögerungsfunktion eines PPS sind strukturelle Barrieren, disponierbare Barrieren und Wachpersonal, deren primäre Aufgabe es ist, einen Angreifer auf dem Weg zu dem Ziel seines Angriffs zu verzögern. Dadurch vergrößern sie die zur Umsetzung von Reaktionsmaßnahmen verfügbare Zeit. Maßnahmen, die verzögernd wirken, werden innerhalb des geschützten Bereiches um das Objekt umgesetzt, da sie nur so einen Einfluss auf die verfügbare Zeit zwischen Detektion und Reaktion haben können. Als sekundärer Effekt geht von Verzögerungsmaßnahmen auch eine abschreckende Wirkung auf einen potentiellen Angreifer aus.

Ausmaß der Verzögerung

Für das Ausmaß der Verzögerung, welches durch umgesetzte Maßnahmen erzielt wird, ist Ursprung und Vorgehensweise der jeweils betrachteten Bedrohungen entscheidend. Darüber hinaus können auch Motivation, Organisationsgrad und Grad der Gewaltanwendung des Angreifers einen Einfluss auf die Verzögerung gegenüber einer spezifischen Bedrohung und sollten beachtet werden.

Abgrenzung von Verzögerung und Reaktion

Bei der Zuordnung von Maßnahmen zur Verzögerungs- oder Reaktionsfunktion kommt es im PPS Konzept, wie es bei Garcia (2006; 2007) beschrieben ist, zu Über-

schneidungen. So wird etwa Wachpersonal sowohl der Verzögerung als auch der Reaktion zugeordnet. Um eine scharfe Abgrenzung der beiden Funktionen und eine Zuordnung von Maßnahmen zu den Funktionen zu ermöglichen, soll deshalb hier eine abweichende Abgrenzung von Verzögerung und Reaktion vorgenommen werden. Zur Verzögerung tragen all diejenigen Maßnahmen an Bord des Schiffes und gegebenenfalls in seiner Umgebung, sowie alle Eigenschaften des Schiffes selber bei, die einen Angreifer ohne aktive Handlung der Besatzung bei seinem Angriff verzögern. Damit ist eine Verzögerung auch gegeben, wenn keine Detektion des Angriffs stattfindet. Dies trägt jedoch nicht zu der primären Funktion der Verzögerung bei. Maßnahmen und Eigenschaften stellen zusammen die Verzögerungselemente des Schiffes dar. Diese Verzögerungselemente beschreiben Hindernisse, Herausforderungen und Schwierigkeiten, mit welchen der Angreifer auf dem Weg zu seinem Ziel fertig werden muss. Der Reaktion werden all diejenigen Maßnahmen zugerechnet, die ein aktives Handeln durch die Besatzung voraussetzen. Entsprechend kann eine Reaktion nur erfolgen, nachdem der Angriff detektiert ist. Außerdem können Reaktionsmaßnahmen nur umgesetzt werden, wenn die dazu nötigen Ressourcen im Moment des Angriffes vorhanden sind. Wohingegen Verzögerungsmaßnahmen im Vorfeld eines Angriffes vorbereitet werden ohne die Ressourcen im Angriffsfall zusätzlich zu belasten. [18] Die Reaktionsmaßnahmen können dabei auch vollständig oder partiell darauf ausgelegt sein, den Angriff zu verzögern und ihn nicht direkt abzuwehren.

Maßnahmen zur Verzögerung an Bord eines Schiffes

Maßnahmen zur Verzögerung können nur an Bord des Schiffes oder in unmittelbarer Umgebung des Schiffes umgesetzt werden, da sich keine Maßnahmen auf dem offenen Meer, welches die Umgebung des Schiffes darstellt, implementieren lassen. Eine gesonderte Betrachtung von Maßnahmen zur Verzögerung von latenten Bedrohungen wird nicht vorgenommen. Im Moment der Detektion einer latenten Bedrohung wird diese zur evidenten Bedrohung, wodurch die gleichen Verzögerungselemente relevant werden wie für die evidente Bedrohung.

Einzelindikator Verzögerung

> Der **Einzelindikator Verzögerung** bildet ab, in welchem Maß die Eigenschaften des Schiffes und Maßnahmen, die an dem Schiff umgesetzt sind, in der Lage sind, das Vorankommen eines Angreifers zu verzögern bzw. zu behindern. Er orientiert sich an der Wahrscheinlichkeit eine ausreichende Verzögerung aufzubieten, um den Angriff neutralisieren zu können.

Abschreckende Wirkung von Verzögerungsmaßnahmen

Die Ausprägung der Verzögerungselemente hat immer auch einen Einfluss auf ein Abschrecken eines Angriffs bevor dieser begonnen hat und auf einen möglichen Abbruch des Angriffs nach dessen Beginn. Dies sind wichtige Bestandteile der Verzögerungsfunktion des Schiffes. Sie sollen aber nicht explizit mit dem Indikator abgebildet werden, da eine Bewertung der Wirkung der Verzögerungselemente auf die Entscheidung eines Angreifers nur schwer und wenn, dann mit großer Unsicherheit, zu bestimmen ist.

[18] Aufgrund der begrenzten Anzahl an Besatzungsmitgliedern an Bord können diese nur eine begrenzte Anzahl von Reaktionsmaßnahmen zeitgleich umsetzen. Die einem Angriff vorgelagerte Einrichtung von Verzögerungsmaßnahmen kann sukzessiv erfolgen und ist damit weniger stark beschränkt.

4.3.3. Reaktion

Reaktion

Die dritte Funktion, die in einem Einzelindikator abgebildet werden soll, ist die Reaktion. Sie beinhaltet alle Maßnahmen, mit denen einer Sicherheitsverletzung begegnet wird. Unterschieden wird zwischen einer unmittelbaren und einer verzögerten Reaktion.

Verzögerte Reaktion

Ob eine verzögerte Reaktion, die dem Angriff nachgelagert stattfindet, auch im Zusammenhang mit Bedrohungen für ein Schiff sinnvoll ist und wie diese aussehen sollte, ist im Rahmen des Risikomanagements zu überprüfen. Da die verzögerte Reaktion jedoch nicht direkt an der Wahrscheinlichkeit der Abwehr eines Angriffes selber beteiligt ist, findet sie keine Berücksichtigung für den Vulnerabilitätsindikator.

Unmittelbare Reaktion

Eine zentrale Bedeutung für die Bewertung der Vulnerabilität nimmt indessen die unmittelbare Reaktion ein. Sie beinhaltet alle Maßnahmen, die bei Eintreten eines Angriffes auf das Schiff umgesetzt werden. Voraussetzung für die Umsetzung einer unmittelbaren Reaktion ist eine erfolgreiche Detektion der Sicherheitsverletzung. Die unmittelbare Reaktion lässt sich weiter unterteilen in eine interne und eine externe Reaktion. Die interne Reaktion wird durch die Besatzung oder entsprechendes Sicherheitspersonal an Bord aufgebracht. An einer externen Reaktion sind Individuen aus dem äußeren Umfeld des Schiffes beteiligt, die erst im Fall eines Angriffes zum Schiff kommen und vor Ort eine Reaktion umsetzen.

Untergliederung der unmittelbaren Reaktion in verzögernde und neutralisierende Reaktion

Abweichend vom PPS Konzept, wie es bei Garcia (2006; 2007) beschrieben ist, kann die Reaktion sowohl eine verzögernde Wirkung als auch eine neutralisierende Wirkung haben. Welche Reaktionsmaßnahmen geeignet sind einen Angriff zu neutralisieren bzw. zu verzögern ist abhängig von Ursprung, Vorgehen, Motivation, Organisationsgrad und Grad der Gewaltanwendung des Angreifers unter dem betrachteten Bedrohungsszenario. Deshalb wird die Reaktion anhand von zwei Einzelindikatoren ermittelt. Einer misst die verzögernde Wirkung der Reaktionsmaßnahmen - der andere bewertet wie lange es dauert bis eine neutralisierende Reaktion aufgebraucht werden kann.

Einzelindikator verzögernde Reaktion

> Der **Einzelindikator verzögernde Reaktion** bildet ab, inwiefern die Reaktionsmaßnahmen, die an einem Schiff umgesetzt werden, in der Lage sind das Vorankommen eines Angreifers zu verzögern bzw. zu behindern. Damit wird bestimmt, in welchem Umfang die verzögernde Reaktion dazu beiträgt das für ein Neutralisieren des Angriffs nötige Ausmaß an Verzögerung aufzubieten.

Einzelindikator neutralisierende Reaktion

> Der **Einzelindikator neutralisierende Reaktion** bildet ab, mit welcher zeitlichen Verzögerung eine für die Neutralisation des Angriffes ausreichende Reaktion an dem Schiff erwartet werden kann. Was eine neutralisierende Reaktion darstellt, ist je nach Bedrohungsszenario unterschiedlich und muss ermittelt werden.

Beispielsweise lässt sich ein terroristisch motivierter Angriff nur durch einen umfangreichen Einsatz von Gewalt neutralisieren, wenn angenommen wird, dass die Angreifer bereit sind ihr eigenes Leben bei dem Angriff zu opfern. Demgegenüber kann bei einem Angriff zum Zweck der persönlichen Bereicherung, was für Angriffe durch Pira-

ten unterstellt wird, auch bei einer im Vergleich wesentlich geringeren Gegenwehr des Schiffes schon eine Kapitulation der Angreifer erfolgen, wenn diese nicht gewillt sind eine Verletzung der eigenen Gesundheit zu riskieren.

Abschreckende Wirkung von Reaktionsmaßnahmen

Genauso wie von Verzögerungselementen und Detektionsmaßnahmen geht auch von den Reaktionsmaßnahmen eine abschreckende Wirkung aus und sie können den Angreifer zu einem Abbruch des Angriffs bewegen. Für die Messung der Reaktion soll jedoch das Augenmerk auf der Wirkungskraft der Reaktion selbst liegen und nicht darauf ob sie auf einen Angreifer abschreckend wirkt.

4.4. Datenerfassung für die Einzelindikatoren

Vorgehen für die Datenerfassung

Jedes Schiff, für das die Einzelindikatoren bestimmt werden sollen, hat eine andere physische Beschaffenheit. Dementsprechend muss ein Konzept zur Bestimmung der Einzelindikatoren eine gewisse Flexibilität aufweisen, um der Diversität der untersuchten Objekte gerecht zu werden. Folgendes Vorgehen berücksichtigt die Vielgestaltigkeit der betrachteten Objekte und ermöglicht das Bestimmen der Einzelindikatoren auf einem praktikablen, praxisnahen Niveau:

1. Entwicklung von qualitativen Skalen für die Bewertung der Vulnerabilität jedes selektierten Einzelindikators gegenüber einem spezifischen Bedrohungsszenario.
2. Formulierung von Einflussfaktoren / Aspekten, die bei der Einordnung eines Objektes innerhalb einer Skala relevant sind und betrachtet werden müssen.
3. Verifizierung von Skalen und Einflussfaktoren im Rahmen von Experteninterviews.

Mithilfe der Skalen und Einflussfaktoren ist es anschließend möglich ein Schiff, in den für die Vulnerabilität relevanten Gesichtspunkten, zu bewerten, etwaige Schwachstellen zu identifizieren und daraus abgeleitet Maßnahmen zur Verringerung der Vulnerabilität auszuwählen.

4.4.1. Skalen

Qualitative Skalen zur Bewertung der Einzelindikatoren

Die Ausprägung der Einzelindikatoren eines Schiffes wird anhand einer qualitativen Skala bewertet. Entsprechend muss für jeden Einzelindikator eine an den zu untersuchenden Kontext angepasste Skala entwickelt werden. Zusammen bildet dieses Set von Skalen die Grundlage der Vulnerabilitätsbewertung

Anpassen der Skalen an jeweilige Bedrohung

Da die Vulnerabilität gegenüber verschiedenen Bedrohungen untersucht wird, ist zu prüfen, ob ein Set von Skalen für die Bewertung unter allen untersuchten Bedrohungen geeignet ist. Die Bedrohungen können sich unter Umständen im Hinblick auf spezifische Charakteristika wie dem Vorgehen, der Motivation und dem Leistungsvermögens unterscheiden. Sollte dies der Fall sein, gilt es, ein spezifisches Set von Skalen angepasst an die jeweils betrachtete Bedrohung zu entwickeln.

Gestaltung der Skalen

Jede Skala besteht aus mehreren ordinalen Levels, in welche das untersuchte Objekt einzuordnen ist. Um die Zuordnung der Objekte zu erleichtern, wird den jeweiligen Levels eine Beschreibung zugewiesen. Die Anzahl der Levels ist auf fünf beschränkt. Diese reichen von vernachlässigbar mit der Ausprägung 1 (nahezu keine signifikante Wirksamkeit) über moderat mit der Ausprägung 3 bis zu umfangreich mit der Aus-

prägung 5 (sehr weitreichende Wirksamkeit). Die Entscheidung, die Skalen in fünf Levels untergliedern, ist ein Kompromiss zwischen einer potentiell höheren Genauigkeit bei der Einordnung je mehr Levels angeboten werden und der gleichzeitigen Zunahme der Komplexität und Unübersichtlichkeit für den Anwender, womit eine geringere Praktikabilität einhergeht (Fletcher 2005, S.1577). Die Gestaltung der Skalen und die Verbalisierung der fünf ordinalen Ausprägungen orientiert sich an den von Greenberg u.a. (2006, S.146-148, 151-152) entwickelten Skalen zur Bewertung von Intentionen und Fähigkeiten der Angreifer, Vulnerabilität des angegriffenen Objektes und Auswirkungen des Angriffs im Zusammenhang von terroristischen Anschlägen im maritimen Umfeld.

4.4.2. Einflussfaktoren

Einflussfaktoren bei der Zuweisung innerhalb einer Skala

Bei der Zuweisung eines Schiffes zu einem Level innerhalb einer der erstellten Skalen sind verschiedene, für den jeweiligen untersuchten Kontext charakteristische, Einflussfaktoren zu berücksichtigen. In Kapitel 3.2 wurde besprochen, dass physische, technische, operative und organisatorische Aspekte sowie etwaige umgesetzte Gegenmaßnahmen ausschlaggebend für die Vulnerabilität des Schiffes sind. Sie bilden die Ausgangsbasis für die Bestimmung der Einflussfaktoren für die Einzelindikatoren.

Identifikation relevanter Einflussfaktoren

Bei der Identifikation relevanter Einflussfaktoren wird zunächst auf die verfügbare Literatur zurückgegriffen. Die zweite Quelle zur Ermittlung von Einflussfaktoren stellen Experteninterviews dar. Sollten Diskrepanzen zwischen den aus der Literatur abgeleiteten und von den Experten genannten Einflussfaktoren auftreten, werden diese mit den Experten diskutiert. Als Ergebnis entsteht eine Liste von Einflussfaktoren, die bei der Einordnung eines Objektes in einer Einzelindikator-Skala für ein betrachtetes Bedrohungsszenario relevant sind.

4.4.3. Verifizierung

Verifizierung von Skalen und Einflussfaktoren im Rahmen von Experteninterviews

Zur Verifizierung der Einflussfaktoren sowie der Skalen, mit deren Hilfe die Ausprägung der Einzelindikatoren für ein Schiff bestimmt wird, werden Experteninterviews durchgeführt. Experteninterviews, als teilstrukturierte Interviews, sind insbesondere dann sinnvoll, wenn es darum geht die relevanten Einflussfaktoren in einem Untersuchungszusammenhang zu ermitteln und zu identifizieren (Cooper u. a. 2008, S.386).

Festlegen wer als ein Experte in Frage kommt

Wer als ein Experte für ein Interview in Frage kommt, wird von der Person, welche die Untersuchung durchführt, festgelegt. Als Orientierung nennen Meuser & Nagel (1991, S.443), dass eine Person als Experte in Frage kommt,

- wenn sie „ (…) in irgendeiner Weise Verantwortung trägt für den Entwurf, die Implementierung oder die Kontrolle einer Problemlösung oder“,
- wenn sie „ (…) über einen privilegierten Zugang zu Informationen über Personengruppen oder Entscheidungsprozesse verfügt.“

Im hier untersuchten Zusammenhang sind dies Personen, die durch ihre berufliche Stellung über relevante Informationen, spezielle Kenntnisse und praxisnahe Erfahrung aus dem Kontext der Phänomene der Piraterie und des maritimen Terrorismus sowie deren Bekämpfung verfügen. Für dieses Arbeitspapier wurden Sicherheitsbe-

auftragte von international agierenden Reedereien sowie Mitarbeiter von Firmen, die Beratungsleistungen im Bereich der maritimen Sicherheit anbieten, befragt.

Ablauf der Experteninterviews

Zur Durchführung der teilstrukturierten Interviews wurde ein Leitfaden erstellt, der gewährleistet, dass jedes Interview vergleichbar abläuft und jeweils alle relevanten Bereiche abgefragt werden. Folgender Ablauf war für die Interviews vorgesehen:

1. Einleitende Fragen, um bisherige Berührungspunkte und Erfahrungen der Experten mit den Phänomenen der Piraterie und des maritimen Terrorismus abzufragen, um so ihren Wissenstand einordnen zu können.
2. Vorstellen des Konzeptes zur Einordnung der Vulnerabilität eines Schiffes anhand der Funktionen Detektion, Verzögerung und Reaktion (verzögernd, neutralisierend). Erfragen der Expertenmeinung zu diesem Konzept.
3. Darstellung der untersuchten Bedrohungsszenarien, für die die Vulnerabilität des Schiffes ermittelt werden soll.
4. Zentrale Frage: Welche Einflussfaktoren (Eigenschaften des Schiffes, Prozesse an Bord, umgesetzte Technologien) sind unter den untersuchten Bedrohungsszenarien relevant für die Bewertung der verschiedenen Einzelindikatoren. Welches Gewicht haben die jeweiligen Einflussfaktoren aus Sicht der Experten.
5. Diskussion von Einflussfaktoren, die im Kontext dieser Arbeit als relevant betrachtet werden, aber nicht von den Experten genannt wurden.
6. Zuletzt Vorstellen der Skala anhand derer die Ausprägung der Einzelindikatoren unter Bezug auf die Einflussfaktoren gemessen wird. Diskussion über die Eignung der Skala, insbesondere in Bezug auf die ausformulierten Abstufungen der Skalen.

Der Gesprächsverlauf der Interviews wurde mit einer Tonbandaufnahme protokolliert und transkribiert. Anschließend sind die Gesprächsprotokolle den Interviewten vorgelegt worden. Dies geschah um ihnen zu ermöglichen, über das Interview hinaus auf besonders relevante Aspekte hinzuweisen und Stellung zu nehmen. Dem Anliegen der Gesprächspartner nach Anonymität wurde entsprochen. [19]

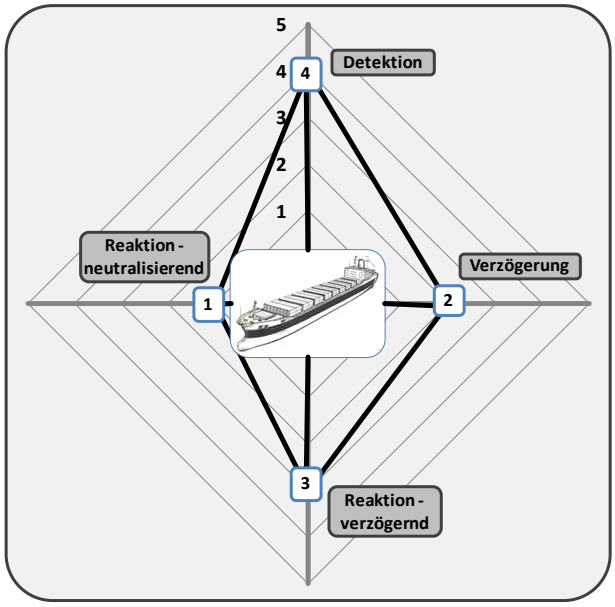
4.5. Visualisierung und Interpretation

Visualisierung des Vulnerabilitätsindikators

Es wird eine exemplarische, graphische Visualisierung des Vulnerabilitätsindikators für verschiedene, hypothetische Schiffe entworfen. Um die Ausprägung der vier Einzelindikatoren in einem Diagramm übersichtlich zusammenzufassen, wird auf ein Netzdiagramm zurückgegriffen. Wie beispielhaft in Abb. 6 dargestellt, ist jeder Einzelindikator auf einer Achse abgebildet, wobei die Stärke der Ausprägung nach außen hin zunimmt. Die gewählte Darstellungsform erlaubt nicht nur einen schnellen Überblick über die Ausprägung der Einzelindikatoren, sondern ermöglicht es auch verschiedene Schiffe untereinander zu vergleichen.

[19] Die Interviewskripte liegen im persönlichen Archiv der Autoren. Falls Nachfragen diesbezüglich bestehen, ist es möglich, nach Rücksprache mit dem jeweilig Interviewten, die Inhalte einzusehen.

Abb. 6: Beispiel der Darstellung der Ausprägung der Einzelindikatoren eines Schiffes



Neben der Visualisierung des Vulnerabilitätsindikators ist außerdem dargestellt wie eine Ermittlung der Einzelindikatoren unter dem entwickelten Vorgehen aussieht und wie sich daraus, anhand der Ausprägung der Einzelindikatoren, die Interpretation der Vulnerabilität ergibt.

Beispielhafte Darstellung des entwickelten Vorgehens und Interpretation der Vulnerabilität

5. Anwendung des Vulnerabilitätsindikatorkonzeptes

Dieser Abschnitt zeigt die Umsetzung des zuvor dargestellten Konzepts zur Entwicklung eines Vulnerabilitätsindikators für eine Gruppe von Bedrohungsszenarien, die eine vergleichbare Vorgehensweise aufweisen. Dabei werden die für die Einzelindikatoren entwickelten Bewertungsskalen dargestellt und die identifizierten Einflussfaktoren beschrieben. Anschließend folgen eine Darstellung der Ergebnisse der Experteninterviews sowie eine Anwendung des Konzeptes auf drei fiktive Schiffe.

Anwendung des Vulnerabilitätsindikator-konzeptes

5.1. Bedrohungsszenarien

Aufgrund der Anzahl und Vielfältigkeit der zu den Phänomenen Piraterie und maritimer Terrorismus diskutierten Bedrohungsszenarien[20], wird im Folgenden das Konzept nur für eine Auswahl umgesetzt. Es wird jedoch davon ausgegangen, dass eine Umsetzung des Konzepts für alle denkbaren Szenarien möglich ist. Diese Arbeit betrachtet Bedrohungsszenarien, die ein Entern des Schiffes durch einen Angreifer beinhalten. Hierunter fallen die aktuell insbesondere vor der Küste Somalias auftretenden Vorfälle von Piraterie, bei denen ein Schiff entführt wird, um ein Lösegeld vom Schiffseigner zu erpressen. Außerdem zählen dazu verschiedene Szenarien des maritimen Terrorismus, bei denen die Kontrolle über ein Schiff übernommen wird, um es anschließend bei einem Anschlag einzusetzen. Folgende Vorgehensweise der Angreifer wird angenommen:

Betrachtete Bedrohungsszenarien beinhalten ein Entern des Schiffes durch einen Angreifer

[20] Siehe hierzu die in Kapitel 3.1 angeführten Autoren.

Angreifer nähern sich dem fahrenden Schiff mit mehreren kleinen schnellen Booten auf hoher See. Befinden sie sich innerhalb der Reichweite ihrer Waffen, eröffnen sie das Feuer auf das Schiff. Sobald sie zum Schiff aufgeschlossen haben, versuchen sie es zu entern, wobei Enterhaken und Enterleitern zum Einsatz kommen. Nach erfolgreichem Entern des Schiffes, ist das Ziel der Angreifer die Besatzung in ihre Gewalt zu bringen und die Kontrolle über das Schiff zu übernehmen.

5.2. Einzelindikatoren und Einflussfaktoren

5.2.1. Detektion

Skala zur qualitativen Bewertung der Detektion

Für evidente Bedrohungen soll bewertet werden, wie wahrscheinlich es ist, einen Angreifer / Angriff bei der Annäherung an das Schiff zu detektieren. Tabelle 5 stellt die Skala dar, welche zur Messung Detektionsfähigkeit gegenüber einer Bedrohung, bei der das Schiff auf offener See geentert werden soll, herangezogen wird.

Tabelle 5: Skala zur Bewertung der Detektionsfähigkeit gegenüber einer evidenten Bedrohung

BEWERTUNG	DETEKTION EINES SICH NÄHERNDEN ANGREIFERS
1 (gering)	Das Erkennen einer Annäherung ist nicht zu erwarten.
2	Das Erkennen einer Annäherung an das Schiff ist auch in unmittelbarer Umgebung des Schiffes wahrscheinlich.
3	Das Erkennen einer Annäherung in unmittelbarer Umgebung ist zuverlässig zu erwarten, in signifikanter Entfernung ist es möglich.
4	Das Erkennen einer Annäherung ist in unmittelbarer Umgebung des Schiffes sehr zuverlässig zu erwarten, in signifikanter Entfernung ist es wahrscheinlich.
5 (hoch)	Das Erkennen einer Annäherung ist in signifikanter Entfernung zum Schiff zuverlässig zu erwarten.

Einflussfaktoren auf die Detektionsfähigkeit

Folgende Einflussfaktoren sind relevant für die Detektionsfähigkeit und müssen bei der Bewertung des Einzelindikators Detektion – Evidente Bedrohung berücksichtigt werden:

Radar – Das Radar des Schiffes ist die zentrale Einrichtung, wenn es darum geht die weitere Umgebung des Schiffes zu überwachen. Entscheidend für die Detektionsfähigkeit ist, ob die Signatur sich nähernder Angreifer vom Radar abgebildet wird.

Optische Überwachung – Optische Überwachung spielt in der näheren Umgebung des Schiffes eine große Rolle und ist ausschlaggebend für die Alarmbewertung. Die Alarmbewertung hat die Aufgabe, zu beurteilen, ob von einem Objekt in der Umgebung des Schiffes tatsächlich eine Bedrohung ausgeht. Findet eine optische Überwachung statt, erhöht sich die Detektionsfähigkeit. Verschiedene Technologien wie Nachtsichtgeräte, Scheinwerfer oder Ferngläser können die optische Überwachung unterstützen.

Anzahl der Personen, die an der Detektion beteiligt sind – Die Anzahl der Personen (Besatzungsmitglieder oder externe Sicherheitskräfte), die an der Detektion potentieller Bedrohungen beteiligt sind. Je höher die Anzahl, desto eher wird eine Bedro-

hung erkannt. Dementsprechend wirkt sich die Anzahl positiv auf die Detektionsfähigkeit aus.

Sorgfalt bei der Umgebungsüberwachung – Sowohl für die Radarüberwachung als auch für die optische Überwachung hat die Sorgfalt, mit der die Überwachung durchgeführt wird, einen großen Einfluss darauf, ob und wann eine Bedrohung erkannt wird. Je größer die Sorgfalt eingeschätzt wird, desto besser ist die Detektionsfähigkeit.

Schulung der Besatzung – Eine Schulung der Besatzung wie potentielle Angriffe zu erkennen sind, erhöht die Wahrscheinlichkeit einer erfolgreichen Detektion und demnach die Detektionsfähigkeit.

Technische Einrichtungen – Beispielsweise Sensoren, Videoüberwachung oder Algorithmen, die Radarsignaturen automatisch auswerten, können die Detektionsfähigkeit verbessern. [21]

Externe Aufklärung – Aufklärung durch Dritte (Handelsschiffe, Marineschiffe, Luftaufklärung, Satellitenüberwachung) und Weitergabe von Informationen zu möglichen / tatsächlichen Bedrohungen. Wenn Informationen zu Gefahren an ein Schiff weitergegeben werden, erhöht dies die Detektionsfähigkeit.

5.2.2. Verzögerung

Skala zur qualitativen Bewertung der Verzögerung

Mit dem Einzelindikator Verzögerung soll bewertet werden in welchem Maß die Eigenschaften des Schiffes und Maßnahmen, die an dem Schiff umgesetzt sind, in der Lage sind das Vorankommen eines Angreifers zu verzögern bzw. zu behindern. Für die hier untersuchte Bedrohung, bei der das Schiff auf offener See geentert werden soll, wurde die in Tabelle 6 dargestellte Skala entwickelt.

Tabelle 6: Skala zur Bewertung der Verzögerung gegenüber einer evidenten Bedrohung

BEWERTUNG	GRAD DER VERZÖGERUNG DER ERREICHT WERDEN KANN
1 (gering)	Eine Verzögerung ist nicht zu erwarten oder die Gestaltung des Schiffes begünstigt den Angreifer bei einem Entern des Schiffes.
2	Eine Verzögerung ist nur in geringem Umfang zu erwarten. Ein an Bord Kommen ist geringfügig erschwert.
3	Eine merkliche Verzögerung ist zu erwarten. Ein an Bord Kommen ist deutlich erschwert.
4	Eine signifikante Verzögerung ist zu erwarten. Ein an Bord Kommen ist erheblich erschwert.
5 (hoch)	Der Angriff kann sehr umfangreich verzögert werden. Ein an Bord Kommen ist nahezu auszuschließen.

Einflussfaktoren auf die Verzögerungsfähigkeit

[21] Eine Analyse von schiffsbezogenen Sicherheitstechnologien zur Detektion von Angriffen im Kontext von Piraterie und maritimem Terrorismus findet sich bei Blecker u. a. (2011a).

Folgende Einflussfaktoren sind bei der Bewertung der Verzögerungsfähigkeit einer Bedrohung, bei der ein sich in Fahrt befindliches Schiff geentert werden soll, von Bedeutung und müssen berücksichtigt werden:

Relative Geschwindigkeit – Die Differenz der Geschwindigkeit des Angreifenden und des Angegriffenen. Je geringer die relative Geschwindigkeit ist, desto länger braucht ein Angreifer, um nach Detektion des Angriffs die verbleibende Distanz zwischen ihm und dem Schiff zu überbrücken. Eine geringe relative Geschwindigkeit wirkt sich positiv auf die Verzögerungsfähigkeit aus.

Absolute Geschwindigkeit – Die Geschwindigkeit des angegriffenen Schiffes. Je höher diese ist, desto schwieriger ist es für einen Angreifer das Schiff zu entern. Eine hohe absolute Geschwindigkeit wirkt sich positiv auf die Verzögerungsfähigkeit aus.

Freibord – Der Abstand zwischen Wasser und Reling des Schiffes. Je höher dieser ist, desto schwerer ist es das Schiff zu entern. Dementsprechend ist die Verzögerungsfähigkeit umso größer, je höher der Freibord ist.

Genereller Aufbau der Reling – Der Aufbau des Schiffes und der Reling etwa Luken, die nahe der Wasserlinie liegen und ein Entern des Schiffes erleichtern. Ist der Aufbau anfällig gegenüber einem Entern, hat dieses einen negativen Einfluss auf die Verzögerungsfähigkeit.

Genereller Aufbau an Bord – Soll abbilden wie einfach es für einen Angreifer ist sich an Bord zurechtzufinden und voranzukommen. Verschiedene Maßnahmen können ergriffen werden, um dies zu erschweren. Ist es für einen Angreifer schwierig an Bord voranzukommen, hat dies einen positiven Einfluss auf die Verzögerung.

Äußere Umstände – Seegang, Sichtverhältnisse etc. können einen Angreifer dabei behindern zum Schiff aufzuschließen und es zu entern. Damit wirken sich die äußeren Umstände positiv auf die Verzögerungsfähigkeit aus.

Technische Einrichtungen – Werden geeignete Technologien eingesetzt, erhöhen sie die Verzögerungsfähigkeit.[22]

5.2.3. Reaktion

Reaktion teilt sich auf in verzögernd und neutralisierend

Bei der Reaktion werden zwei Aspekte, eine verzögernde Reaktion des Schiffes und eine neutralisierende Reaktion des Schiffes, betrachtet und bewertet. Um eine Wirkung auf einen Angreifer zu erzielen, setzen beide eine erfolgreiche Detektion des Angriffs voraus.

VERZÖGERNDE REAKTION

Skala zur qualitativen Bewertung der verzögernden Reaktion

Mit dem Einzelindikator verzögernde Reaktion wird bewertet in welchem Maß die am Schiff umgesetzten Reaktionsmaßnahmen in der Lage sind, einen Angreifer bei seinem Vorhaben zu verzögern. Für die hier betrachtete Bedrohung, des Enterns des Schiffes auf offener See, kann die verzögernde Reaktion anhand der in Tabelle 7 dargestellten Skala bewertet werden.

[22] Eine Analyse von schiffsbezogenen Sicherheitstechnologien zur Verzögerung von Angriffen im Kontext von Piraterie und maritimem Terrorismus, Hamburg findet sich bei Blecker u. a. (2011b).

Tabelle 7: Skala zur Bewertung der verzögernden Reaktion gegenüber einer evidenten Bedrohung	
BEWERTUNG	**VERZÖGERNDE REAKTION**
1 (gering)	Keine verzögernde Reaktion auf einen Angriff ist möglich oder die Reaktion hat kaum merkliche Auswirkungen auf das Vorankommen des Angreifers.
2	Eine verzögernde Reaktion auf einen Angriff kann in geringem Maß umgesetzt werden. Die dadurch erzielte Verzögerung ist gering.
3	Die verzögernde Reaktion auf einen Angriff ist durchschnittlich. Die dadurch erzielte Verzögerung ist durchschnittlich.
4	Die verzögernde Reaktion auf einen Angriff ist signifikant. Die dadurch erzielte Verzögerung ist signifikant.
5 (hoch)	Die verzögernde Reaktion auf einen Angriff ist sehr umfangreich. Ein an Bord Kommen ist nahezu auszuschließen.

Einflussfaktoren auf die verzögernde Reaktion

Folgende Einflussfaktoren sind bei der Bewertung der verzögernden Reaktion gegenüber einer Bedrohung für ein Schiff, das sich in Fahrt befindet und geentert werden soll, von Bedeutung und müssen berücksichtigt werden:

Geschwindigkeit – Eine Erhöhung der Geschwindigkeit sobald ein Angriff detektiert ist. Dies vergrößert die Zeit, die ein Angreifer benötigt, um zum Schiff aufzuschließen und erschwert ein Entern. Kann die Geschwindigkeit gesteigert werden, ist dies positiv für die verzögernde Reaktion.

Manöver –Im Fall eines Angriffs können Manöver des Schiffes, beispielsweise leichte Ruderbewegungen, ein Entern des Schiffes erschweren. Werden Manöver durchgeführt, erhöht sich damit die verzögernde Reaktion.

Gegenmaßnahmen der Besatzung – Die Besatzung kann weitere Gegenmaßnahmen im Fall eines Angriffes durchführen, wobei sie sich am Schiff befindlicher Einrichtungen, etwa der Löschwasseranlage, bedient. Werden Gegenmaßnahmen umgesetzt, erhöht sich damit die verzögernde Reaktion.

Technische Einrichtungen – Sind zusätzliche technische Einrichtungen an Bord des Schiffes umgesetzt, können diese im Fall eines Angriffes zum Einsatz gebracht werden. Stehen entsprechende Technologien zur Verfügung, erhöht sich damit die verzögernde Reaktion. [23]

Schulung der Besatzung – Sind die Besatzungsmitglieder geschult für die Durchführung von Gegenmaßnahmen im Fall eines Angriffs, erhöht sich die Wirksamkeit dieser Maßnahmen. Dies hat einen positiven Einfluss auf die verzögernde Reaktion.

Sicherheitskräfte – Sind Sicherheitskräfte an Bord, können diese Reaktionsmaßnahmen im Angriffsfall durchführen. Dies hat einen positiven Einfluss auf die verzögernde Reaktion.

[23] Eine Analyse von schiffsbezogenen Sicherheitstechnologien zur Reaktion auf Angriffe im Kontext von Piraterie und maritimem Terrorismus findet sich bei Blecker u. a. (2012).

NEUTRALISIERENDE REAKTION

Skala zur qualitativen Bewertung der neutralisierenden Reaktion

Der Einzelindikator neutralisierende Reaktion bildet ab, mit welcher zeitlichen Verzögerung eine für die Neutralisation des Angriffes ausreichende Reaktion an dem Schiff umgesetzt werden kann. Es wird, im Einklang mit den interviewten Experten, angenommen, dass, um den Angriff zu neutralisieren, gegenüber einem bewaffneten Angreifer nur eine Reaktion durch bewaffnete Sicherheitskräfte wirkungsvoll ist. Die in Tabelle 8 dargestellte Skala wird zur Bewertung der neutralisierenden Reaktion herangezogen.

Tabelle 8: Skala zur Bewertung der neutralisierenden Reaktion gegenüber einer evidenten Bedrohung

BEWERTUNG	NEUTRALISIERENDE REAKTION
1 (gering)	Keine neutralisierende Reaktion ist zu erwarten.
2	Eine neutralisierende Reaktion kann erst nach großer Verzögerung stattfinden.
3	Eine neutralisierende Reaktion kann erst nach gewisser Verzögerung stattfinden.
4	Eine neutralisierende Reaktion kann nach kurzer Zeit stattfinden.
5 (hoch)	Eine neutralisierende Reaktion ist ohne Zeitverzögerung vor Ort möglich.

Einflussfaktoren auf die neutralisierende Reaktion

Die folgenden Einflussfaktoren gilt es im Zuge der Bewertung der neutralisierenden Reaktion zu betrachten:

Externe Sicherheitskräfte – Sollte ein Schiff angegriffen werden, kommen externe Kräfte dem Schiff zu Hilfe. Hier ist zu bestimmen wie lange es dauert bis eine ausreichende Anzahl von Sicherheitskräften das Schiff erreicht.

Interne Sicherheitskräfte – Interne Kräfte befinden sich im Fall eines Angriffs an Bord des Schiffes. Da folglich nur mit einer marginalen Zeitverzögerung zu rechnen ist bis sie gegen den Angriff vorgehen können, ist in erster Linie zu prüfen, ob die internen Sicherheitskräfte hinlänglich ausgerüstet und in ausreichender Anzahl vor Ort sind, um eine neutralisierende Reaktion umsetzen zu können. Ist dies nicht der Fall, müssen auch bewaffnete Sicherheitskräfte der verzögernden Reaktion zugeordnet werden.

5.3. Diskussion der Experteninterviews

Diskussion der Experteninterviews

Es wurden Interviews zur Verifizierung des Konzeptes, mithilfe dessen die Vulnerabilität eines Schiffes abgebildet wird, durchgeführt. Hierbei sind die Einflussfaktoren sowie die Skalen zur Bestimmung der Einzelindikatoren mit den Experten besprochen worden. Tabelle 9 beinhaltet eine Charakterisierung der Interviewpartner. Alle Interviews fanden Anfang 2011 statt.

Tabelle 9: Charakterisierung der Interviewpartner		
	UNTERNEHMEN	**INTERVIEWTE PERSON**
A	Beratungsunternehmen	Direktor Maritime Security Division
B & C	Reederei	Geschäftsführer & Company Security Officer
D	Reederei	Leiter Versicherungsabteilung

Experten bestätigen das entwickelte Konzept

Alle Experten bestätigen die Eignung des entwickelten Konzepts zur Beschreibung der Vulnerabilität und stimmen der Zusammenstellung an oben angeführten Einflussfaktoren zu. Dabei sind in den Interviews verschiedene Aspekte von den Experten besonders betont worden, auf die im Folgenden eingegangen wird.

PPS Konzept als Grundlage des Vulnerabilitätsindikators

Experte A betrachtet explizit dieselben Bereiche – Detektion, Verzögerung, Reaktion – wie in dieser Arbeit bei einer Bewertung der Vulnerabilität eines Schiffes. B, C und D kennen das Konzept wonach Detektion, Verzögerung und Reaktion die Vulnerabilität maßgeblich beeinflussen und wenden es implizit an.

Expertenaussagen zu: Risikobewertung

Eine qualitative Risikobewertung wird von A vorgenommen. Dabei finden nur die Faktoren Typ des Schiffes[24], Geschwindigkeit des Schiffes und Freibord des Schiffes Berücksichtigung. Die Aufnahme weiterer Faktoren in die Risikobewertung sieht A als wünschenswert. Als problematisch wird dabei der Zugang zu entsprechenden Informationen und deren Beurteilung betrachtet. Bei möglichen weiteren Faktoren handelt es sich, nach Aussage von A, größtenteils um schwer objektiv zu bewertende „Soft Facts“. D sieht eine zunehmende Notwendigkeit, sich mit dem Thema der Risikobewertung auseinanderzusetzten. Er gibt an, dass dies inzwischen standardmäßig von den Versicherungen umgesetzt wird. Bei regelmäßigen Treffen zwischen Reedern und Versicherern wird dazu eine Reihe verschiedener Einflussfaktoren abgefragt. Auf diesen Faktoren basiere die Risikobewertung, woraus sich die Versicherungsprämien der Schiffe ableiten. Neben Schiffstyp, Geschwindigkeit und Freibord nennt D Schutzräume, Nato-Draht, Dummys, General Arrangement Pläne[25], Trainingsintervalle der Besatzung, Ablaufpläne an Bord des Schiffes, Sicherheitsteams und Zustand der Schiffe als Faktoren, die von Seiten der Versicherungen abgefragt und in die Risikobewertung aufgenommen werden.

Expertenaussagen zu: Detektion

Im Zusammenhang mit der Detektion wurde von allen Experten darauf hingewiesen, dass, aufgrund der inzwischen zahlenmäßig sehr geringen Besatzung an Bord, kaum die Möglichkeit besteht zusätzliche Besatzungsmitglieder für eine Überwachung des Schiffsumfeldes abzustellen. Zu diesem Zweck bietet sich der Einsatz von Sicherheitsteams an. Radar wird von B, C sowie D in seiner Bedeutung für die Detektion, wegen der Probleme bei der Darstellung kleiner Schiffe, als eher gering eingeschätzt. Zentral für die Detektion ist nach ihrer Ansicht die visuelle Überwachung des Schiffsumfeldes.

Expertenaussagen zu: Schulung der Besatzung

Ein wesentlicher Punkt ist nach Meinung aller Experten die Schulung der Besatzung, mit der die Wirksamkeit von Detektions- und Reaktionsmaßnahmen sichergestellt

[24] Im Sinn von: Bulk-Carrier, Containerschiff, Liquid-Gas-Carrier etc..

[25] Eine technische Zeichnung, die den Aufbau des Schiffes erkennen lässt.

und erhöht werden kann. A sieht in diesem Zusammenhang als weiteren Faktor, wie erfahren oder „robust“[26] eine Besatzung ist.

Expertenaussagen zu: Externe Detektion

Eine externe Detektion schätzt A als wirkungsvoll ein, sieht aber Schwierigkeiten darin, wer für die Kosten der Informationsbeschaffung aufkommt und in welcher Form die generierten Informationen den betroffenen Schiffen zur Verfügung gestellt werden.

Expertenaussagen zu: Genereller Aufbau der Reling

Hinsichtlich des Einflussfaktors „Genereller Aufbau der Reling“ weist A auf die Bedeutung von Luken und Öffnungen hin, die sich nahe der Wasseroberfläche befinden. D ergänzt, dass von Seiten der Versicherungen standardmäßig nach Plänen des Schiffsaufbaus gefragt wird, welche in die Risikobewertung einfließen. Nach Aussage von B und C wissen die Mitarbeiter an Bord am besten wo sich die besonders vulnerablen Bereiche des Schiffes befinden und wie sie am besten zu sichern sind.

Expertenaussagen zu: Bewaffnete Sicherheitskräfte

Alle Experten weisen darauf hin und kritisieren, dass noch immer keine Lösung hinsichtlich der Frage von bewaffneten Sicherheitskräften an Bord von Schiffen unter deutscher Flagge in Sicht ist.[27] Dies könnte A zufolge sogar zu einer Ausweitung des Risikos führen. Denn Piraten könnten deutsche Schiffe als besonders attraktive Ziele betrachten, da hier nicht mit Sicherheitsteams an Bord zu rechnen ist und es sich damit um vergleichsweise wenig geschützte Schiffe handelt. B und C sowie D sehen bewaffnete Sicherheitskräfte, trotz der rechtlich nicht geklärten, unsicheren Lage, inzwischen als Standard in der Praxis an. D weist in dem Zusammenhang auf die damit einhergehenden Risiken aufgrund von ungeklärten Versicherungsfragen hin. Wird etwa bei einem Schusswechsel die Ladung beschädigt, könnte die Deckung eines solchen Schadens von den Ladungshaftpflichtversicherern abgelehnt werden, woraus sich entsprechend Risiken für den Schiffseigner ergeben. Laut B und C geht es aktuell sogar soweit, dass von Seiten der Besatzung die Forderung nach bewaffneten Sicherheitskräften an Bord besteht. Wird dem nicht nachgekommen, sind die Besatzungsmitglieder nicht bereit durch die von Piraterie betroffenen Gebiete zu fahren. Alle Experten sind der Meinung, dass letztendlich nur bewaffnete Sicherheitskräfte an Bord einen wirksamen Schutz gegenüber den evidenten Bedrohungen bieten. Dies wird aus Sicht von B und C zusätzlich dadurch verschärft, dass in der jetzigen Situation die Zeit bis zum Eintreffen von externen Sicherheitskräften in den von Piraterie betroffenen Regionen zu lang ist. Die Experten unterstreichen dabei jedoch auch, dass der Einsatz von bewaffneten Sicherheitskräften an Bord nicht zu einer Vernachlässigung der Bereiche Detektion und Verzögerung führen darf.

Expertenaussagen zu: Maritimer Terrorismus

Gefahren durch maritimen Terrorismus sieht A zurzeit nicht, stimmt aber darin überein, dass dennoch eine Relevanz des Phänomens besteht, weil mit potentiell katastrophalen Auswirkungen bei Eintreten eines Bedrohungsszenarios zu rechnen ist. A erwartet von Terroristen eine höhere Entschlossenheit bei einem Angriff, sieht aber dennoch bewaffnete Kräfte als wirkungsvolle Reaktion an.

[26] Mit dem Ausdruck „robust“ bezieht sich A hier etwa auf eine militärische Vorbildung der Besatzung, die sich in einem entschlosseneren Vorgehen im Angriffsfall niederschlägt und damit einen Einfluss auf die Erfolgswahrscheinlichkeit des Angriffs hat.

[27] Zur Diskussion der rechtlichen Situation sei verwiesen auf König & Salomon (2011).

Alle Experten geben zu bedenken, dass bei allen Abwehrmaßnahmen an Bord eines Schiffes mit einer Anpassung der Angriffstaktik im Laufe der Zeit zu rechnen ist.

Abwehrmaßnahmen führen zu Anpassungsreaktion bei Angreifern

A weist ausdrücklich auf die aus seiner Sicht bestehende Wirksamkeit der Abschreckung bei der Verteidigung eines Schiffes hin. So finden bei der Verteidigung von Piratenangriffen vermehrt Gewehr-Dummys Verwendung. A beschreibt den Ablauf einer bewaffneten Reaktion in den folgenden vier Schritten: (1) Bewaffnung zeigen, (2) Warnschuss in die Luft, (3) Warnschuss vor den Bug, (4) gezielter Schuss auf Angreifer. Die ersten beiden Stufen reichen (aktuell) aus, um Piraten dazu zu bewegen ihren Angriff abzubrechen. D bestätigt dieses, weist aber darauf hin, dass es durchaus zu einer Eskalation der Situation kommen könnte, bei der ein Warnschuss in die Luft nicht mehr ausreichen würde.

Expertenaussagen zu: Wirksamkeit von Abschreckungsmaßnahmen

Neben der in dieser Arbeit betrachteten unmittelbaren Reaktion betont A die Bedeutung des Themas verzögerte Reaktion im Sinne von Krisenmanagement, Verhandlungsführung und Lösegeldübergabe, die im Anschluss an den Angriff beginnt.

Expertenaussagen zu: Verzögerte Reaktion

5.4. Visualisierung der Einzelindikatoren und Interpretation der Vulnerabilität

In diesem Abschnitt soll eine Veranschaulichung des entwickelten Konzeptes anhand hypothetischer Daten erfolgen. [28] Alle Annahmen und Ausprägungen in diesem Abschnitt sind fiktiv und die daraus geschlossenen Bewertungen rein hypothetisch. Wird das Konzept für die Ermittlung der Vulnerabilität realer Schiffe in der Praxis umgesetzt, sollten alle Bewertungen und Einschätzungen von Experten mit umfangreichen Kenntnissen und Erfahrungen in den betrachteten Zusammenhängen vorgenommen werden.

Veranschaulichung des Vulnerabilitätsindikators

Zunächst wird eine Bedrohung ausgewählt, für die eine Bestimmung der Vulnerabilität vorgenommen werden soll. Als Bedrohungsszenario wird ein Entern des Schiffes auf offener See ausgewählt. Das von der Bedrohung betroffene Objekt wird in für die Bereiche Detektion, Verzögerung und Reaktion relevanten Einflussfaktoren charakterisiert. Hieraus wird eine Bewertung der Ausprägung der Einzelindikatoren abgeleitet, besprochen und visualisiert. Zuletzt findet eine Abschätzung der Vulnerabilität des Objektes insgesamt gegenüber der betrachteten Bedrohung statt.

Angenommene Bedrohung

Es werden drei hypothetische Objekte – ein schnelles Containerschiff mit einem hohen Freibord, ein Mehrzweckfrachter mit mittlerer Geschwindigkeit und mittlerem Freibord und ein Very Large Crude Carrier (VLCC)[29] mit geringer Geschwindigkeit und geringem Freibord – untersucht. In Tabelle 10 sind diese Schiffe hinsichtlich einer Auswahl von Einflussfaktoren beschrieben, anhand derer die Bewertung der Einzelindikatoren des Vulnerabilitätsindikators vorgenommen wird. Teilweise wird dabei Bezug genommen auf Technologien zur Verringerung der Vulnerabilität, wie sie bei Blecker u. a. (2011a), Blecker u. a. (2011b) und Blecker u. a. (2012) dargestellt sind.

Drei hypothetische Schiffe

[28] Ein analoges Vorgehen findet sich bei Pate-Cornell & Guikema (2002, S.10–13) und McGill (2007, S.1274–1277), die damit die von ihnen entwickelten Konzepte in ihrer Umsetzung anhand von hypothetischen Daten veranschaulichen.

[29] Große Öltanker die gewöhnlich etwa 2 Millionen Barrel Öl transportieren, werden als VLCC bezeichnet (Stopford 2009, S.xxiv).

Tabelle 10: Auswahl von Einflussfaktoren und deren Ausprägung für drei fiktive Schiffe			
	Containerschiff	**Mehrzweckfrachter**	**VLCC**
Detektion			
Radar	Navigationsradar	Navigationsradar	Navigationsradar
Besatzungsmitglieder im Ausguck	1 Besatzungsmitglied	1 Besatzungsmitglied	2 Besatzungsmitglieder
Sorgfalt bei der Umgebungsüberwachung	Gering	Hoch	Hoch
Schulung der Besatzung	-	Besatzung geschult	Besatzung geschult
Technische Einrichtungen	-	-	Yachtradar am Heck
Verzögerung			
Absolute Geschwindigkeit	Hoch	Mittel	Gering
Freibord	Hoch	Mittel	Gering
Genereller Aufbau der Reling	Neutral	Anfällig	Anfällig
Technische Einrichtungen	-	-	Reling und Schiffsaufbau sind umfassend gehärtet, umfangreicher Einsatz von Stacheldraht
Reaktion - verzögernd			
Manöver	Nicht vorgesehen	Vorgesehen und trainiert	Vorgesehen und trainiert
Gegenmaßnahmen Besatzung	Nicht vorgesehen	Ja	Ja
Sicherheitskräfte	(der neutralisierenden Reaktion zugerechnet)	Ja, unbewaffnet	Nein
Schulung Besatzung	Nein	Ja	Ja
Technische Einrichtungen	-	Wasserkanonen, Reiz-, Rauch-, Blend- und Schockmittel	Schutzraum, Vessel Controll Blocking System
Reaktion - neutralisierend			
Externe Sicherheitskräfte	Nicht zu erwarten	In deutlicher Entfernung	In geringer Entfernung
Interne Sicherheitskräfte	Ja, bewaffnet	(der verzögernden Reaktion zugerechnet)	Nein

Bewertung der Vulnerabilität anhand der beschriebenen Einflussfaktoren

Ist die Ausprägung von relevanten Einflussfaktoren für ein betrachtetes Schiff, wie in Tabelle 10 beispielhaft dargestellt, ermittelt, kann aufbauend die Bewertung der Einzelindikatoren vorgenommen werden. Hierbei kommen die Skalen zur Bewertung der Einzelindikatoren zum Einsatz. Je nachdem wie die Einflussfaktoren ausgeprägt sind, wird das Schiff in eine der 5 Stufen der Skala eingeordnet. Eine hypothetische Bewertung der Einzelindikatoren aufgrund der oben dargestellten Ausprägung der Einfluss-

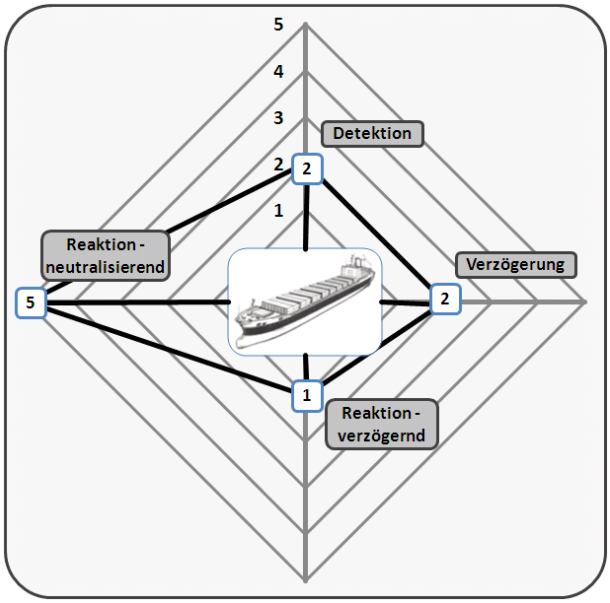
faktoren ist in Tabelle 11 zu sehen. Im Anschluss wird für die drei Schiffe argumentiert, worin sich diese Bewertung begründet.

Tabelle 11: Ausprägung der Einzelindikatoren für drei fiktive Schiffe				
	Detektion evidente Bedrohung	**Verzögerung**	**Reaktion verzögernd**	**Reaktion neutralisierend**
Containerschiff	2	2	1	5
Mehrzweckfrachter	3	1	4	2
VLCC	4	3	4	4

Einzelindikatoren für hypothetisches Containerschiff

Das **Containerschiff** hat einen Wert von zwei für die Detektion, da zwar Radar und Ausguck vorhanden sind und überwacht werden, jedoch die Sorgfalt der Überwachung als gering angenommen ist. Die hohe Geschwindigkeit und der hohe Freibord wirken sich positiv auf die Verzögerung aus. Ohne Maßnahmen, die ein Entern erschweren, wird der Verzögerung dennoch ein vergleichsweise geringer Wert von zwei zugewiesen. Dem Einzelindikator "verzögernde Reaktion" wird der geringste Wert von eins gegeben, denn es sind keine technischen Einrichtungen implementiert oder operative Maßnahmen vorgesehen. Außerdem ist die Besatzung nicht für den Fall eines Angriffs geschult. Angesichts der an Bord befindlichen Sicherheitskräfte wird neutralisierende Reaktion mit fünf bewertet. In Abb. 7 ist eine mögliche Visualisierung der Einzelindikatoren für das Containerschiff dargestellt.

Abb. 7: Einzelindikatoren für ein fiktives Containerschiff



Vulnerabilität des Containerschiffes insgesamt moderat

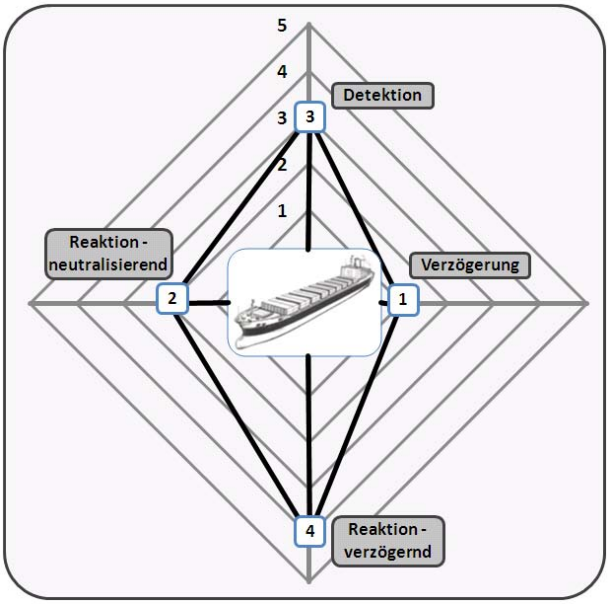
Trotz der als sehr hoch eingeschätzten neutralisierenden Reaktion, ist die Vulnerabilität des Containerschiffes als moderat anzusehen. Dies resultiert aus den geringen Werten der anderen Einzelindikatoren. Ohne eine vorhergehende Detektion und ausreichende Verzögerung kann auch eine umfangreiche neutralisierende Reaktion nicht zu einer erfolgreichen Abwehr eines Angriffs beitragen. Die Implementierung

von Maßnahmen in den Bereichen Detektion sowie Verzögerung bzw. verzögernde Reaktion würde die Vulnerabilität verringern.

Einzelindikatoren für hypothetischen Mehrzweckfrachter

Der **Mehrzweckfrachter** hat einen Wert von drei für die Detektion. Hierin spiegelt sich die, im Vergleich zum Containerschiff, als hoch angesehene Sorgfalt der Besatzung bei den Überwachungsprozessen wider. Eine mittlere Geschwindigkeit, ein mittlerer Freibord und eine Reling, die ein Entern erleichtert, ohne Maßnahmen zur Härtung haben zur Folge, dass ein Entern vergleichsweise einfach möglich ist. Entsprechend wird die Verzögerung mit eins bewertet. Für die verzögernde Reaktion wird dem Mehrzweckfrachter ein hoher Wert von vier zugewiesen. Dies begründet sich in der Schulung der Besatzung, die, unterstützt durch unbewaffnetes Sicherheitspersonal an Bord, umfangreiche Maßnahmen im Fall eines Angriffs umsetzt und dabei auf verschiedene technische Einrichtungen zurückgreifen kann. Da externe Sicherheitskräfte sich in deutlicher Entfernung zum Schiff befinden, wird angenommen, dass eine neutralisierende Reaktion erst nach großer Verzögerung stattfinden kann, was in einem Wert der neutralisierenden Reaktion von zwei resultiert. In Abb. 8 ist eine mögliche Visualisierung der Einzelindikatoren für den Mehrzweckfrachter dargestellt.

Abb. 8: Einzelindikatoren für einen fiktiven Mehrzweckfrachter



Vulnerabilität des Mehrzweckfrachter insgesamt überdurchschnittlich

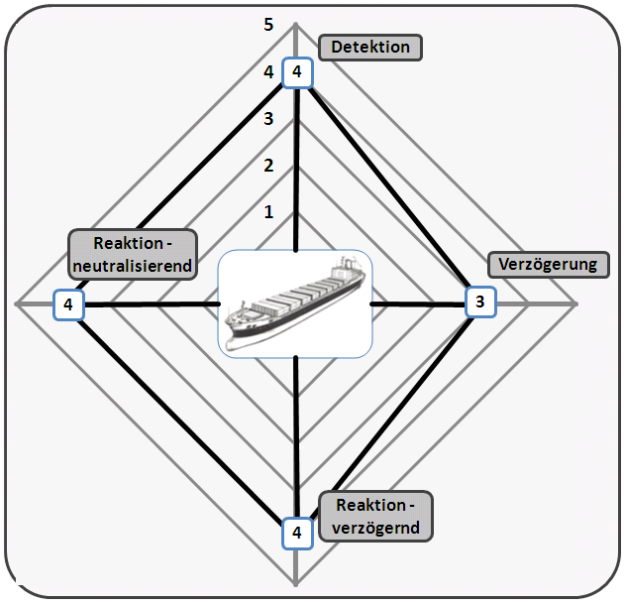
Die Vulnerabilität des Mehrzweckfrachters gegenüber einem Angriff durch Piraten ist insgesamt als überdurchschnittlich bis moderat anzusehen. Positiv wirken sich zwar die Werte für Detektion und verzögernde Reaktion aus, allerdings ist die Inhomogenität der Einzelindikatoren hinderlich für eine bessere Bewertung der Vulnerabilität.

Einzelindikatoren für hypothetischen VLCC

Der **VLCC** hat von den hypothetischen Schiffen den höchsten Wert von vier für die Detektion aufgrund des zusätzlichen Besatzungsmitgliedes, welches für die Detektion abgestellt ist, und eines Yachtradars, das eine Überwachung der vom Navigationsradar nicht abgedeckten Bereiche ermöglicht. Für den VLCC wird die geringste Geschwindigkeit und der geringste Freibord angenommen. Die Bewertung für die Verzögerung ist mit drei dennoch moderat aufgrund der umfangreichen Maßnahmen zur Härtung von Reling und Schiffsaufbau. Der vorhandene Schutzraum, die Vorrichtung

zur Blockierung des Schiffsantriebes sowie eine für den Fall eines Angriffs geschulte Besatzung resultieren in einem Wert von vier für die verzögernde Reaktion. Für die neutralisierende Reaktion wird angenommen, dass sie nach kurzer Zeit am Schiff greift, da externe Sicherheitskräfte in geringer Entfernung verfügbar sind. Deshalb wird ein Wert von vier vergeben. In Abb. 9 ist eine mögliche Visualisierung der Einzelindikatoren für den VLCC dargestellt.

Abb. 9: Einzelindikatoren für einen fiktiven VLCC



Vulnerabilität des VLCC insgesamt unterdurchschnittlich

Obwohl der VLCC - mit geringer Geschwindigkeit und geringem Freibord - von den drei Schiffen am anfälligsten gegenüber einer Bedrohung durch ein Entern ist, kann aufgrund der verschiedenen umgesetzten Maßnahmen an Bord insgesamt die Vulnerabilität des Schiffes als unterdurchschnittlich angesehen werden. Sehr positiv wirkt sich dabei der Umstand aus, dass externe Sicherheitskräfte schneller bei einem Angriff reagieren können, als (Marine-)kräfte, die erst zur Hilfe eilen müssen.

6. Fazit

Erhebliche Risiken für einen Reeder aufgrund von Piraterie und maritimem Terrorismus

Mit Angriffen auf Schiffe durch Piraten oder maritime Terroristen geht ein erhebliches finanzielles Risiko für betroffene Reedereien einher. Die Handhabung dieser Risiken findet im Rahmen eines Risikomanagementprozesses statt.

Risiko-Assessment identifiziert und bewertet bestehende Risiken

Um zu einem erfolgreichen Risikomanagement beizutragen, wurde in diesem Arbeitspapier zunächst das Risiko-Assessment für Bedrohungen, die im Zusammenhang mit Piraterie und maritimem Terrorismus bestehen, dargestellt. Hierbei wurde das Vorgehen bei der Identifikation und Messung von bestehenden Risiken beschrieben.

Risikoverminderung verlangt ein umfassendes Verständnis der Vulnerabilität des Schiffes

Sind Risiken identifiziert und bewertet, gilt es anschließend festzulegen wie im darauf folgenden Schritt der Risikosteuerung mit ihnen umgegangen wird. Hier besteht für betroffene Reedereien eine Möglichkeit in der Strategie der Risikoverminderung durch den Einsatz von geeigneten Technologien. Sind diese Technologien an Bord implementiert, tragen sie zu einer Verringerung der Vulnerabilität des Schiffes und damit auch zu einer Verringerung des Risikos insgesamt bei. Um diese Strategie um-

zusetzen, ist ein umfassendes Verständnis darüber notwendig, welche Faktoren einen Einfluss auf die Vulnerabilität eines Schiffes haben und wie das Zusammenspiel dieser Faktoren gestaltet ist.

Vulnerabilitätsindikator bildet Vulnerabilität ab

Das Ziel dieses Arbeitspapiers bestand darin, dieses Verständnis über die Vulnerabilität eines Schiffes zu erweitern und die Faktoren, welche die Vulnerabilität maßgeblich beeinflussen zu identifizieren. Das Arbeitspapier entwickelt ein Konzept, das eine Messung der Vulnerabilität ermöglicht und damit die Grundlage für eine erfolgreiche Risikoverminderung darstellt. Es wurde ein qualitativer Indikator konstruiert, der die Vulnerabilität des Schiffes anhand verschiedener Kriterien abbildet.

Physical Protection System als Ausgangspunkt für die Entwicklung des Vulnerabilitätsindikators

Den Ausgangspunkt für die Entwicklung des Vulnerabilitätsindikators bildet das Konzept des Physical Protection System. Nach diesem Ansatz sind an einer erfolgreichen Abwendung einer Bedrohung drei Funktionen beteiligt: der Angriff muss (1) detektiert werden, (2) eine ausreichende Verzögerung des Angriffs erreicht werden und (3) eine angemessene Reaktion auf den Angriff umgesetzt werden. Im Rahmen von Expertengesprächen wurde die Eignung dieses Konzeptes für die Bewertung der Vulnerabilität eines Schiffes bestätigt.

Einzelindikatoren zu Detektion, Verzögerung und Reaktion bilden die Vulnerabilität eines Schiffes ab

Entsprechend der Funktionen des Physical Protection System sind die Einzelindikatoren Detektion, Verzögerung und Reaktion definiert, an die Gegebenheiten im maritimen Umfeld angepasst und für ein Schiff beschrieben worden. Zusammengenommen bilden sie die Vulnerabilität des Schiffes ab. Der Einzelindikator Detektion zeigt an, wie wahrscheinlich es ist einen Angriff auf das Schiff zu identifizieren. Der Einzelindikator Verzögerung zeigt an, in welchem Umfang das Vorankommen eines Angreifers ohne eine aktive Handlung der Besatzung verzögert werden kann. Reaktion teilt sich in die Bereiche verzögernde und neutralisierende Reaktion. Verzögernde Reaktion zeigt an, inwiefern aktive Maßnahmen der Besatzung in der Lage sind das Vorankommen eines Angreifers zu behindern. Neutralisierende Reaktion bildet ab, mit welcher zeitlichen Verzögerung eine für die Neutralisation des Angriffes ausreichende Reaktion am Schiff umgesetzt wird. Je besser diese Einzelindikatoren für ein betrachtetes Schiff ausgeprägt sind, desto höher ist die Wahrscheinlichkeit einen Angriff erfolgreich abzuwenden und dementsprechend geringer die Vulnerabilität des Schiffes.

Messung der Einzelindikatoren mithilfe von Skalen und Einflussfaktoren

Die Messung der Einzelindikatoren erfolgt anhand von Skalen, in welche die Ausprägung der abgebildeten Eigenschaft eines spezifischen Schiffes eingeordnet wird. Bei der Einordnung gilt es verschiedene Aspekte der Konstruktion, der technischen Ausstattung und des operativen Betriebes des Schiffes zu berücksichtigen. Diese Aspekte, hier als Einflussfaktoren auf die Einzelindikatoren bezeichnet, müssen bestimmt und beschrieben werden. Das Vorgehen bei der Messung der Einzelindikatoren wurde im Rahmen von Expertengesprächen auf seine Eignung in der Praxis überprüft.

Ausarbeitung des Konzepts für Bedrohungsszenarien, die ein Entern des Schiffes durch einen Angreifer beinhalten

Das entwickelte Konzept des Vulnerabilitätsindikators wurde für eine Gruppe von Bedrohungsszenarien, die ein Entern des Schiffes durch einen Angreifer beinhalten, ausgearbeitet. Hierbei wurden zunächst Skalen beschrieben, anhand derer die Bewertung der Einzelindikatoren unter Bezugnahme auf die Einflussfaktoren, vorgenommen wird. Als zweites galt es die im Zusammenhang dieser Bedrohung relevanten Einflussfaktoren zu identifizieren und zu beschreiben. So ist unter anderem die

Schulung der Besatzung ein zentraler Einflussfaktor auf den Einzelindikator „Detektion“. Geschwindigkeit und Freibord sind Einflussfaktoren auf den Einzelindikator „Verzögerung“. Die von der Besatzung im Angriffsfall eingeleiteten Gegenmaßnahmen sind ein Einflussfaktor für den Einzelindikator „verzögernde Reaktion“. Für den Einzelindikator „neutralisierende Reaktion“ ist zu berücksichtigen, in welcher Entfernung zum Angriffsort sich externe Sicherheitskräfte befinden. Zur Verifizierung des ausgearbeiteten Konzeptes, sind Einflussfaktoren und Skalen mit einer Reihe von Experten diskutiert worden, welche seine Zweckmäßigkeit bestätigt haben. Um die Anwendung des entwickelten Konzeptes für die Praxis zu verdeutlichen, wurde es zuletzt für drei hypothetische Schiffe beispielhaft angewandt.

Der Vulnerabilitätsindikator ermöglicht es gezielt Technologien auszuwählen, welche das Risiko für ein Schiff verringern

Wird mithilfe des Indikators bestimmt, dass die Vulnerabilität eines Schiffes gegenüber einem Bedrohungsszenario ein akzeptables Niveau übersteigt, kann sie durch den Einsatz von zur Sicherheit beitragenden Technologien verringert werden. Ein Katalog entsprechender Technologien für die Bereiche Detektion, Verzögerung und Reaktion findet sich bei Blecker u. a. (2011a), Blecker u. a. (2011b) und Blecker u. a. (2012).

Weiterer Forschungsbedarf: Ausweitung auf andere Bedrohungsszenarien

Dieses Arbeitspapier betrachtet nur Bedrohungsszenarien, die ein Entern des Schiffes durch einen Angreifer beinhalten. Um bei einer Risikobetrachtung Anwendung zu finden, muss das Konzept des Vulnerabilitätsindikators auf andere Bedrohungsszenarien, die im Zusammenhang mit Piraterie und maritimem Terrorismus relevant sind, ausgeweitet werden. Weiter sollte die Vorgehensweise der Angreifer bei einem Angriff zu einer ausführlichen, schrittweisen Darstellung ausgeweitet werden. Diese ist insbesondere für die Einschätzung der Wirksamkeit der zur Sicherheit beitragenden Technologien gegenüber einem Angriff notwendig.

Weiterer Forschungsbedarf: Detaillierung der Einflussfaktoren

Desweiteren besteht bezüglich der identifizierten Einflussfaktoren Bedarf für weitere Untersuchungen. Zum einen sollten die Einflussfaktoren detaillierter ausgearbeitet werden und zum anderen muss ermittelt werden, welches Gewicht die einzelnen Einflussfaktoren bei der Bestimmung der jeweiligen Einzelindikatoren innehaben. Dies könnte im Rahmen einer ausgeweiteten Expertenbefragung stattfinden.

Weiterer Forschungsbedarf: Untersuchung der Risikoelemente Gefahr und Auswirkungen

In dieser Untersuchung wird nur auf eins der drei Risikoelemente eingegangen, die Vulnerabilität. Der Reeder muss bei seiner Entscheidung, welche Strategie er zur Risikosteuerung verfolgt, jedoch auch die anderen beiden Elemente, Gefahr und Auswirkungen, mit berücksichtigen. Als eine Erweiterung dieser Untersuchung ist es folglich angebracht ein Konzept zu entwickeln, das eine Bestimmung von Gefahr und Auswirkungen unter Bedrohungsszenarien im Zusammenhang mit Piraterie und maritimem Terrorismus erlaubt.

Literaturverzeichnis

Ayyub, B.M., McGill, W.L. & Kaminskiy, M., 2007. Critical Asset and Portfolio Risk Analysis: An All-Hazards Framework. Risk Analysis: An International Journal, 27(4), S.789–801.

Bartlett, J., 2004. Project risk analysis and management guide 2. Aufl., Buckinghamshire, UK: APM Publishing Limited.

Birkmann, J., 1999. Indikatoren für eine nachhaltige Entwicklung. Raumforschung und Raumordnung, 57(2-3), S.120–131.

Birkmann, J., 2006. Measuring vulnerability to natural hazards: towards disaster resilient societies, Tokyo [u.a.]: United Nations Univ. Press.

Blackwell, C., 2009. The Insider Threat: Combatting the Enemy Within, Cambridgeshire, UK: IT Governance Publishing.

Blecker, T. u. a., 2011a. Analyse von schiffsbezogenen Sicherheitstechnologien zur Detektion von Angriffen im Kontext von Piraterie und maritimem Terrorismus, Hamburg: PiraT-Working Papers on Maritime Security Nr. 9.

Blecker, T. u. a., 2012. Analyse von schiffsbezogenen Sicherheitstechnologien zur Reaktion auf Angriffe im Kontext von Piraterie und maritimem Terrorismus, Hamburg: PiraT-Working Papers on Maritime Security, *im Erscheinen 2012*.

Blecker, T. u. a., 2011b. Analyse von schiffsbezogenen Sicherheitstechnologien zur Verzögerung von Angriffen im Kontext von Piraterie und maritimem Terrorismus, Hamburg: PiraT-Working Papers on Maritime Security Nr. 10.

Böger, M., 2010. Gestaltungsansätze und Determinanten des Supply Chain Risk Managements – Eine explorative Analyse am Beispiel von Deutschland und den USA. Hamburg: TU Hamburg-Harburg.

Burger, A. & Buchhart, A., 2002. Risiko-Controlling, München: Oldenbourg Wissenschaftsverlag.

Chalk, P., 2008. The Maritime Dimension of International Security- Terrorism, Piracy, and Chanllenges for the United States, Santa Monica, CA: RAND Corporation.

Cherchy, L. u. a., 2006. Creating Composite Indicators with DEA and Robustness Analysis: the case of the Technology Achievement Index. Available at: http://www.econ.kuleuven.ac.be/ew/academic/econover/Papers/DPS0603.pdf [Zugegriffen November 24, 2010].

Cooper, D.R., Schindler, P.S. & Blumberg, B., 2008. Business research methods 2. European ed., London [u.a.]: McGraw-Hill Education.

Cox, L.A., 2009. Risk Analysis of Complex and Uncertain Systems, Berlin, Heidelberg: Springer.

Crist, P., 2003. Security in Maritime Transport: Risk Factors and Economic Impact, Paris: OECD.

Duden, 2007. Duden - Das Fremdwörterbuch - Onlineausgabe 9. Aufl., Mannheim: Bibliographisches Institut & F. A. Brockhaus AG.

Ehrhart, H.-G., Petretto, K. & Schneider, P., 2011. Security Governance als Rahmenkonzept für die Analyse von Piraterie und maritimem Terrorismus –Konzeptionelle und Empirische Grundlagen–, Hamburg: PiraT-Working Papers on Maritime Security Nr. 1.

Engerer, H. & Gössler, M., 2011a. Maritimer Terrorismus und Piraterie aus Sicht der deutschen Versicherungswirtschaft Ergebnisse einer Befragung deutscher Transportversicherer, Hamburg: PiraT-Working Papers on Maritime Security Nr. 12.

Engerer, H. & Gössler, M., 2011b. Piraterie und maritimer Terrorismus aus Sicht deutscher Reeder Ergebnisse einer Befragung, Hamburg: PiraT-Working Papers on Maritime Security Nr. 11.

Ferriere, D., Pysareva, K. & Rucinski, A., 2005. Using Technology to Bridge Maritime Security Gaps, Portsmouth: National Infrastructure Institute Center for Infrastructure Expertise.

Fiege, S., 2006. Risikomanagement- und Überwachungssystem nach KonTraG: Prozess, Instrumente, Träger 1. Aufl., Wiesbaden: Deutscher Universitäts-Verlag, GWV Fachverlage GmbH.

Fletcher, W.J., 2005. The application of qualitative risk assessment methodology to prioritize issues for fisheries management. ICES Journal of Marine Science: Journal du Conseil, 62(8), S.1576 –1587.

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

Gallopin, G.C., 1997. Chapter 1 - Introduction. In B. Moldan & S. Billharz, hrsg. Sustainability Indicators - Report of the project on Indicators of Sustainable Development. SCOPE. Scientific Committee On Problems of the Environment. Available at: http://www.icsu-scope.org/downloadpubs/scope58/ch01-introd.html [Zugegriffen November 17, 2010].

GAO, 2005. RISK MANAGEMENT Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure, Washington, D.C.: U.S. Government Accountability Office (GAO).

Garcia, M.L., 2007. Design and Evaluation of Physical Protection Systems 2. Aufl., Amsterdam [u.a.]: Elsevier Butterworth-Heinemann.

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

Geise, T., 2007. Maritimer Terrorismus in Südostasien. Journal of Current Southeast Asian Affairs, (5), S.7–42.

Greenberg, M.D. u. a., 2006. Maritime terrorism : risk and liability, Santa Monica, CA: RAND Corporation.

Gunaratna, R. hrsg., 2003. Terrorism in the Asia Pacific: Threat and Response, Singapore: Times Academic Press,Singapore.

Haimes, Y.Y., 2006. On the Definition of Vulnerabilities in Measuring Risks to Infrastructures. Risk Analysis, 26(2), S.293–296.

Hiete, M. & Merz, M., 2009. An Indicator Framework to Assess the Vulnerability of Industrial Sectors against Indirect Disaster Losses. In J. Landgren & S. Jul, hrsg. Proceedings of the 6th International ISCRAM Conference – Gothenburg, Sweden, May 2009. 6th International ISCRAM Conference – Gothenburg, Sweden, May 2009. Gothenburg.

Jenisch, U., 2010. Piraterie/Terrorismus - Passagierschifffahrt und Terrorismus - Eine unterschätzte Gefahr. MarineForum, (5), S.4–8.

Johnson, D. & Valencia, M.J. hrsg., 2005. Piracy in Southeast Asia : status, issues, and responses, Singapore: ISEAS Publications.

Kaplan, S. & Garrick, B.J., 1981. On The Quantitative Definition of Risk. Risk Analysis, 1(1), S.11–27.

König, D. u. a., 2011. Piraterie und maritimer Terrorismus als Herausforderungen für die Seesicherheit: Objektive Rechtsunsicherheit im Völker-, Europa- und deutschen Recht, Hamburg: PiraT-Working Papers on Maritime Security Nr. 7.

König, D. & Salomon, T.R., 2011. Private Sicherheitsdienste auf Handelsschiffen – Rechtliche Implikationen, Hamburg: PiraT-Working Papers on Maritime Security Nr. 2.

Lave, L., 2002. View Point: Risk Analysis and the Terrorism Problem in Two Parts. Risk Analysis: An International Journal, 22(3), S.403–404.

Lenz, S., 2009. Vulnerabilität Kritischer Infrastrukturen, Bonn: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.

Maclaren, V.W., 1996. Urban sustainability reporting. Journal of the American Planning Association, 62(2), S.184–203.

McGill, W.L., 2008. Critical Asset and Portfolio Risk Analysis for Homeland Security. College Park, Md.: University of Maryland.

McGill, W.L., Ayyub, B.M. & Kaminskiy, M., 2007. Risk Analysis for Critical Asset Protection. Risk Analysis: An International Journal, 27(5), S.1265–1281.

McNicholas, M., 2008. Maritime Security - An Introduction, Oxford: Butterworth-Heinemann.

Meuser, M. & Nagel, U., 1991. ExpertenInterviews - vielfach erprobt, wenig bedacht. In D. Garz & K. Kraimer, hrsg. Qualitativ-empirische Sozialforschung : Konzepte, Methoden, Analysen. Opladen: Westdeutscher Verlag, S. 441–471.

Mildner, S.-A. & Groß, F., 2010. Piraterie und Welthandel: Die wirtschaftlichen Kosten. In S. Mair, hrsg. Piraterie und maritime Sicherheit - Fallstudien zu Afrika, Südostasien und Lateinamerika sowie Beiträge zu politischen, militärischen, rechtlichen und ökonomischen Aspekten. Berlin: SWP Stiftung Wissenschaft und Politik Deutsches Institut für Politik und Sicherheit.

Mischuk, G., 2009. Piraterie in Südostasien, Euskirchen: Amt für Geoinformationswesen der Bundeswehr.

Morral, A.R. & Jackson, B.A., 2009. Understanding the Role of Deterrence in Counterterrorism Security, Santa Monica, CA: RAND Corporation.

Moteff, J., 2005. Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences, Congressional Research Service - The Library of Congress.

Murray-Tuite, P.M. & Fei, X., 2010. A Methodology for Assessing Transportation Network Terrorism Risk with Attacker and Defender Interactions. Computer-Aided Civil and Infrastructure Engineering, 25(6), S.396–410.

OECD, 2008. Handbook on Constructing Composite Indicators - Methodology and User Guide, Paris: Organisation for Economic Co-operation and Development (OECD) Publications Service.

Ong-Webb, G.G. hrsg., 2006. Piracy, Maritme Terrorism and Securing the Malacca Straits, Singapore: Institute of Southeast Asian Studies.

Pate-Cornell, E. & Guikema, S., 2002. Probabilistic Modeling of Terrorist Threats: A Systems Analysis Approach to Setting Priorities Among Countermeasures. Military Operations Research, 7(4), S.5–20.

Petretto, K., 2011. Diebstahl, Raub und erpresserische Geiselnahme im maritimen Raum – Eine Analyse zeitgenössischer Piraterie –, Hamburg: PiraT-Working Papers on Maritime Security Nr. 8.

PWC, 2011. Deutsche Schifffahrt: Land in Sicht - Befragung von 100 Führungskräften der deutschen Hochseereedereien, Hamburg: PricewaterhouseCoopers (PWC).

RAMCAP, 2006. Risk Analysis and Management for Critical Asset Protection - The Framework - Version 2.0, Wachington, D.C.: ASME Innovative Technologies Institute.

Roper, C.A., 1999. Risk management for security professionals, Oxford: Butterworth-Heinemann.

Rosenkranz, F. & Missler-Behr, M., 2005. Unternehmensrisiken erkennen und managen, Berlin/Heidelberg: Springer-Verlag.

Saltelli, A., 2006. Composite Indicators between Analysis and Advocacy. Social Indicators Research, 81(1), S.65–77.

Schneider, P., 2011. Maritimer Terrorismus: Tätergruppen und Anschlagstypen – Eine empirisch-analytische Bestandsaufnahme –, Hamburg: PiraT-Working Papers on Maritime Security Nr. 13.

Sharpe, 2004. Literature Review of Frameworks for Macro-indicators, Ottawa: Centre for the Study of Living Standards.

Stehr, M., 2004. Piraterie und Terror auf See - Nicht-Staatliche Gewalt auf den Weltmeeren 1990 bis 2004 1. Aufl., Berlin: Verlag Dr. Köster.

Stopford, M., 2009. Maritime economics 3rd ed., London [u.a.]: Routledge.

UN WWAP, 2003. 1st UN World Water Development Report: Water for People, Water for Life, Paris, New York and Oxford: United Nations Educational, Scientific and Cultural Organization (UNESCO) and Berghahn Books.

UNODC, 2010. Crime and instability - Case studies of transnational threats, United Nations Office on Drugs and Crime (UNODC).

Viscusi, W.K. & Aldy, J.E., 2003. The Value of a Statistical Life: A Critical Review of Market Estimates Throughout the World. Journal of Risk and Uncertainty, 27(1), S.5–76.

Willis, H.H. u. a., 2005. Estimating Terrorism Risk, Santa Monica, CA: RAND Corporation.

Willis, H.H. u. a., 2007. Terrorism Risk Modeling for Intelligence Analysis and Infrastructure Protection, Santa Monica, CA: RAND Corporation.

Wolf, K. & Runzheimer, B., 2009. Risikomanagement und KonTraG: Konzeption und Implementierung, Gabler Verlag.

Wolke, T., 2009. Risikomanagement 2., vollst. überarb. und erw. Aufl., München: Oldenbourg.