Resilienz maritimer Kritischer Infrastrukturen

Dr.-Ing. habil. Frank Sill Torres[*]

Eine größere Anzahl maritimer Infrastrukturen sind für die Versorgung und das Wohlergehen der Bevölkerung von wesentlicher Bedeutung und gelten daher aus Sicht des Gesetzgebers als Kritische Infrastruktur. Angesichts vielfältiger Bedrohungen wird die Resilienz dieser Systeme – die Fähigkeit, Störereignissen zu widerstehen und sich schnell zu erholen – zunehmend relevant. Der vorliegende Beitrag diskutiert Maßnahmen zur Verbesserung der Resilienz dieser Infrastrukturen.

A. Einleitung

Die Bedeutung maritimer Infrastrukturen für Deutschland ist vielseitig und teils essenziell. Als eine führende Exportnation spielt der Handel über See eine wesentliche Rolle für die deutsche Wirtschaft sowie die Weltwirtschaft insgesamt. Etwa 80 % des globalen Handelsvolumens werden über den Seeweg abgewickelt. Dabei erreichte der Exportwert der Bundesrepublik Deutschland im Jahr 2021 1.375 Milliarden Euro, während der Importwert 1.203 Milliarden Euro betrug[1]. Im Jahr 2023 wurden rund 270 Millionen Tonnen Güter mit einem erheblichen Volumen über das Meer verschifft, was einen wesentlichen Anteil des deutschen Handelsvolumens darstellt[2]. In diesem Kontext sind nicht nur die Häfen, sondern auch wichtige Schiffswege wie der Nord-Ostsee-Kanal von zentraler Bedeutung. Neben der Funktion als Handelsroute ist die maritime Infrastruktur auch wichtiger Teil der Energieversorgung Deutschlands. Ein signifikanter Anteil der Energieproduktion wird durch Offshore-Windparks gewährleistet. Deren ins deutsche Stromnetz einspeisende Anlagen wiesen im Jahr 2022 eine

* Der Verfasser ist Institutsdirektor (komm.) am Deutschen Zentrum für Luft- und Raumfahrt e.V. (DLR), Institut für den Schutz maritimer Infrastrukturen in Bremerhaven.

1 Marinekommando, Jahresbericht 2022 – Fakten und Zahlen zur maritimen Abhängigkeit der Bundesrepublik Deutschland, Hrsg. Marinekommando Rostock, S. 147.

2 Statistisches Bundesamt, Seeverkehr 2023, Wiesbaden.

https://doi.org/10.5771/9783748953494-13 - am 23.01.2026, 02:27:29. https://www.inlibra.com/de/agb - Open Access -

Nennleistung von rund 8,1 Gigawatt auf, was etwa 4 % der Bruttostromerzeugung Deutschlands entsprach[3]. Die Ausbauziele der Bundesregierung sehen bis 2045 eine Erhöhung der Leistung auf mindestens 70 Gigawatt vor, was mehr als 25 % der gesamten Bruttostromerzeugung ausmachen würde[4]. Zudem wird ein erheblicher Anteil des Erdgasverbrauchs über die Nordseepipelines importiert; im Jahr 2022 betrug dieser Anteil etwa 56 % des gesamten Erdgasverbrauchs in Deutschland[5]. Auch im Bereich der digitalen Infrastruktur sind maritime Systeme unverzichtbar. So werden über 95 % des weltweiten Datenverkehrs über Unterseekabel abgewickelt[6].

Aktuelle Ereignisse wie die Angriffe auf Nord Stream und den Baltic Connector verdeutlichen jedoch, dass physische Bedrohungen gegen maritime Infrastrukturen nicht nur theoretischer Natur sind, sondern reale und unmittelbare Risiken darstellen[7]. Der Schutz dieser Infrastrukturen ist daher von größter Relevanz für die Bevölkerung und die nationale Sicherheit. Diese Ereignisse zeigen jedoch auch, wie anspruchsvoll und komplex der Schutz dieser Infrastrukturen ist und dass eine 100%ige Sicherheit kaum erreichbar ist.

Aus diesem Grund gewinnt neben der Gefahrenabwehr das Thema Resilienz zunehmend an Bedeutung. Resilienz beschreibt in diesem Kontext die Fähigkeit von Systemen und Organisationen, Störereignissen zu widerstehen bzw. sich daran anzupassen und dabei die Funktionsfähigkeit zu erhalten oder möglichst schnell wiederzuerlangen.

Das Ziel dieses Beitrags ist es, fachfremden Lesern eine Einführung in das Thema Resilienz maritimer Infrastrukturen zu geben. Dazu wird zunächst ein Überblick über maritime Kritische Infrastrukturen präsentiert (B.), gefolgt von einer Diskussion zu den spezifischen Sicherheitsherausforderungen im maritimen Sektor (C.). Anschließend wird eine Einführung in die Resilienz sozio-technischer Systeme gegeben (D.), aus der Ansätze zur Erhöhung der Resilienz abgeleitet werden (E.).

3 Deutsche WindGuard, Status des Offshore-Windenergieausbaus in Deutschland – Jahr 2023, Varel, S. 3.
4 § 1 WindSeeG.
5 *Hilgers/Busch*, Energie und Rohstoff Erdgas: Verfügbarkeit, Engpässe und Alternativen, Angewandte Geowissenschaften, 2022, S. 27.
6 *Gorden/Jones*, Global Communications Infrastructure: Undersea and Beyond, Center for Space Policy and Strategy, 2022, S. 2.
7 *Liebetrau/Bueger,* International Journal of Critical Infrastructure Protection v. 46 2024, 100683 (100683).

https://doi.org/10.5771/9783748963494-13 - am 23.01.2026, 02:27:29. https://www.inlibra.com/de/agb - Open Access -

B. Maritime Kritische Infrastrukturen

Kritische Infrastrukturen sind Einrichtungen, Systeme oder Teile davon, die für das Funktionieren einer Gesellschaft und ihrer Wirtschaft von entscheidender Bedeutung sind. Ihr Ausfall oder ihre Beeinträchtigung würden erhebliche Auswirkungen auf die öffentliche Sicherheit, das öffentliche und wirtschaftliche Wohl oder die öffentliche Gesundheit haben[8].

In der aktuellen Gesetzgebung zu Kritischen Infrastrukturen (KRITIS) in Deutschland werden acht primäre Sektoren identifiziert, die für die Aufrechterhaltung lebenswichtiger gesellschaftlicher Funktionen entscheidend sind[9]. Diese Sektoren umfassen Energieversorgung, Wasserversorgung, Informations- und Kommunikationstechnologie, Finanz- und Versicherungswesen, Lebensmittelversorgung, Transport und Verkehr, Gesundheitswesen sowie Entsorgung. Innerhalb dieser Sektoren stellen die Betreiber spezifischer KRITIS-Anlagen grundlegende Dienstleistungen bereit, um die kontinuierliche Versorgung der Bevölkerung und deren Wohlergehen zu gewährleisten. Wenn ein Betreiber mit seinen Anlagen die in der KRITIS-Verordnung festgelegten, dienstleistungsbezogenen Schwellenwerte überschreitet, werden diese Anlagen gemäß der Verordnung als Kritische Infrastruktur eingestuft, wodurch der Betreiber zum KRITIS-Betreiber wird. Diese Klassifizierung zieht spezifische rechtliche Verpflichtungen nach sich, die unter anderem die Implementierung adäquater Sicherheitsmaßnahmen, die Meldepflicht von sicherheitsrelevanten Vorfällen und die Durchführung regelmäßiger Prüfungen umfassen. Auf den maritimen Bereich übertragen trifft eine solche Einstufung aktuell u. a. auf folgende Infrastrukturarten zu: Seekabel zur Daten- und Stromübertragung, Gaspipelines, Offshore-Windparks und -Konverterstationen, Liquefied-Natural-Gas-Anlagen, Hafenanlagen (z.B. Umschlaganlagen, Leitzentralen, Hafeninformationssystem) und Verkehrsleitzentralen.[10]

C. Bedrohungen und Vulnerabilitäten

Im Folgenden werden die grundsätzlichen Bedrohungen und Vulnerabilitäten maritimer Infrastrukturen überblicksartig vorgestellt.

8 Vgl. 2008/114/EG, Artikel 2
9 Vgl. §2 (10) BSIG
10 *Voelsen,* Maritime kritische Infrastrukturen, SWP-Studie 2024/S 03, 2024, 7.

https://doi.org/10.5771/9783748963494-13 - am 23.01.2026, 02:27:29. https://www.inlibra.com/de/agb - Open Access -

I. Bedrohungen

Grundsätzlich können Bedrohungen für kritische maritime Infrastrukturen unterteilt werden in Naturgefahren und anthropogene Bedrohungen. Zu den Naturgefahren zählen im maritimen Raum bspw. Sturmfluten, Hochwasser, hoher Wellenschlag, Extremwetter, Blitzschlag oder Seebeben. Vom Menschen ausgehende Bedrohungen können wiederum unterteilt werden in unbeabsichtigte und beabsichtige Bedrohungen. Zu den Ersteren gehören bspw. Arbeitsunfälle und Fehlbedienungen. Das Feld der beabsichtigten anthropogenen Bedrohungen ist ungleich vielfältiger und umfasst Diebstahl, mutwillige Beschädigung, Sabotage, Cyber-Angriffe, Terrorismus und weitere.

II. Vulnerabilitäten

Die Herausforderungen für den Schutz kritischer Infrastrukturen unterscheiden sich im maritimen Raum teils signifikant von denen im terrestrischen Raum. Hierzu gehört insbesondere die räumliche Ausdehnung der zu überwachenden Gebiete. So beträgt die Größe der deutschen Meeresflächen[11] ca. 41.000 km² in der Nordsee und 15.400 km² in der Ostsee, was in etwa der Fläche der deutschen Bundesländer Niedersachsen (47.710 km²) sowie Schleswig-Hollstein (15.804 km²) entspricht. Des Weiteren verfügen auch die Infrastrukturen über eine große Ausbreitung. So können bspw. Offshore Windparks eine Flächengröße von mehr als 100 km² haben, während Pipelines eine Länge von über 1.000 km besitzen können.

Die räumliche Ausdehnung zusammen mit der Tatsache, dass Einsatzkräfte gewöhnlich in Küstennähe bzw. auf Inseln stationiert sind, führt zusätzlich zu langen Interventionszeiten. Diese umfassen bei Luftfahrzeugen oft über 30 min, während bei Wasserfahrzeugen in Stunden gerechnet wird[12]. Dies erschwert maßgeblich eine zeitnahe Reaktion auf bedrohliche Ereignisse.

Ein weiteres Merkmal des Schutzes maritimer Infrastrukturen ist die Multi-Dimensionalität. Das bedeutet, es müssen sowohl die Bereiche Meeresboden (bspw. für Pipelines, Datenkabel), Unterwasser (bspw. für Angriffe durch Unterwasserfahrzeuge), Wasseroberfläche (bspw. für Offshore

11 Jeweils Küstenmeer und Ausschließliche Wirtschaftszone i.S.d. Art. 2, Art. 55 ff. SRÜ

12 Hierbei ist die Vorbereitungszeit der Luftfahrzeuge, welche ebenfalls 30 – 60 min in Anspruch nehmen kann, nicht mit eingerechnet.

https://doi.org/10.5771/9783748963494-13 - am 23.01.2026, 02:27:29. https://www.inlibra.com/de/agb - Open Access -

Windparks und Offshore Plattformen), Luftraum (bspw. für Angriffe durch bzw. gegen Luftwahrzeuge und Drohnen) und der Cyberraum überwacht und geschützt werden.

Weitere Herausforderungen sind die durch das internationale Seerecht grundsätzlich gewährte freie Zugänglichkeit der Meere sowie die schlechte Attributierbarkeit, welche die Identifikation und Verfolgung von Verantwortlichen für illegale oder schädliche Aktivitäten erschwert.

D. Resilienz

Dieser Abschnitt dient der Einführung in das Thema Resilienz sowie der Betrachtung von Fähigkeiten resilienter Systeme.

I. Begriffsdefinition

Es gibt vielfältige Verständnisse von Resilienz. Dies liegt an der langen Entwicklungsgeschichte des Konzepts[13], konstanten Diskussionen über seine Ausgestaltung, bspw. illustriert durch die unterschiedlichen Ansichten von Holling[14] und Pimm[15], sowie die fortlaufenden Anpassungen des Resilienzverständnisses in verschiedenen Forschungsbereichen wie Ökologie[16], Katastrophenmanagement[17] und dem Schutz von Kritischer Infrastrukturen[18]. Daher unterscheidet sich die genaue Bedeutung von Resilienz je nach Fachgebiet und spezifischem Anwendungsbereich. Zu nennen sind hier beispielsweise die Definitionen zur „seismischen Resilienz in Gemeinden"[19], die Hurrikanresilienz von Stromnetzen[20] oder die „Resilienz" i.S.d. Anpassungsfähigkeit von Städten an den Klimawandel[21]. Grundsätzlich ermöglicht jedoch die Resilienzdefinition des Büros der Vereinten Nationen für Katastrophenvorsorge eine grundlegende und weitakzeptierte An-

13 *Alexander*, in Nat. Hazards Earth Syst. Sci. v. 13 2013, 2707 (2708).
14 *Holling*, Annual Review of Ecology, Evolution, and Systematics v. 4 1973, 1 (3).
15 *Pimm*, Nature v. 307 1984, 321 (324).
16 *Carpenter*, Ecosystems v. 4 2001, 765 (770).
17 *Cutter*, Global Environ. Change v. 18 2018, 598 (600).
18 *Poulin*, *Kane*, Reliability Engineering and System Safety v. 216 2021, 107926 (107928).
19 *Bruneau*, Earthquake Spectra v. 19 2003, 733 (740).
20 *Ouyang/Duenas-Osorio*, Structure Safety v. 48 2014, 15 (18).
21 *Brown*, Environmental Urbanization v. 24 2012, 531 (538).

https://doi.org/10.5771/9783748963494-13 - am 23.01.2026, 02:27:29. https://www.inlibra.com/de/agb - Open Access -

näherung[22]. Sie definiert Resilienz als „die Fähigkeit eines Systems, einer Gemeinschaft oder einer Gesellschaft, sich rechtzeitig und effizient den Auswirkungen einer Gefährdung widersetzen, diese absorbieren, sich an sie anpassen, sie umwandeln und sich von ihnen erholen zu können. Eine wichtige Voraussetzung dafür ist die Erhaltung und Wiederherstellung ihrer wesentlichen Grundstrukturen und Funktionen durch Risikomanagement".[23]

II. Fähigkeiten resilienter Systeme

Zentrale Aspekte bei der Betrachtung der Resilienz eines Systems sind dessen Fähigkeiten und die Anwendung von Resilienzprinzipien[24]. Letztere umfassen grundlegende Regeln, Richtlinien oder Ziele, die entscheidend sind, um die Entwicklung und Gestaltung resilienter Systeme zu steuern und eine wesentliche Orientierung für die Auswahl effektiver resilienzsteigernder Maßnahmen bieten[25]. In der Fachliteratur gibt es verschiedene Ansichten zu den essenziellen Systemfähigkeiten eines resilienten Systems[26]. Insbesondere im Bereich kritischer Infrastrukturen werden jedoch häufig drei Systemfähigkeiten hervorgehoben, welche im Folgenden beschrieben werden.

1. Absorptionsfähigkeit

Unter Absorbtionsfähigkeit mag man die Fähigkeit eines Systems verstehen, die initialen negativen Effekte einer Störung zu mindern und dennoch funktionsfähig zu bleiben. Diese Fähigkeit dient der Aufrechterhaltung der Systemkontinuität und umfasst Maßnahmen, die entweder automatisch oder mit minimalem Aufwand wirksam werden können. Dies steht im Gegensatz zu Wiederherstellungs- und Anpassungsfähigkeit, die oft spezifische Maßnahmen erfordern. Im Unterschied zu gezielten Schutzmaßnahmen, die für bestimmte Szenarien konzipiert sind, erhöhen Absorptions-

22 *United Nations Office for Disaster Risk Reduction*, Sendai Framework Terminology on Disaster Risk Reduction, 2016.
23 *Bundesregierung*, Deutsche Strategie zur Stärkung der Resilienz gegenüber Katastrophen, 2022, 17.
24 *Woods*, Reliability Engineering and System Safety v. 141 2015, 5 (6).
25 *Jackson/Ferris*, Systems Engineering v. 16 2013, 152 (155).
26 *Rehak*, International Journal of Critical Infrastructure Protection v. 25 2019, 125 (130).

https://doi.org/10.5771/9783748963494-13 - am 23.01.2026, 02:27:29. https://www.inlibra.com/de/agb - Open Access -

maßnahmen die allgemeine Widerstandsfähigkeit eines Systems gegenüber verschiedenen Störungen.

2. Wiederherstellungsfähigkeit

Die Fähigkeit eines Systems, seine Funktionsleistung nach einer Störung rasch zu regenerieren, ist ein zentrales Element vieler Resilienzdefinitionen. Die Wiederherstellungsfähigkeit bezieht sich auf Maßnahmen, die durchgeführt werden, um die Auswirkungen einer Störung rückgängig zu machen. Dazu gehören bspw. der Einsatz von Reparaturteams, die Instandsetzung beschädigter Komponenten unter Verwendung von Ersatzteilen oder die Beschaffung benötigter Teile. Weitere wesentliche Aspekte sind effektive Notfallpläne, kompetente Notfallreaktionen und die effiziente Zuweisung von Personal und Ressourcen.[27]

3. Anpassungsfähigkeit

Unter Anpassungsfähigkeit versteht man weithin die Fähigkeit eines Systems, sich selbst zu modifizieren, um zukünftigen Störungen effektiv zu begegnen. Dies impliziert, dass das System seine aktuellen Praktiken oder Strategien ändert und aus vergangenen Störungen lernt. Zu den Maßnahmen, die die Anpassungsfähigkeit fördern, gehören die Überarbeitung von Plänen, die Modifikation von Verfahren sowie die Implementierung neuer Werkzeuge, Technologien und Schulungen, die zur Optimierung vor der nächsten Krise erforderlich sind. Die Anpassungsfähigkeit eines Systems wird primär durch soziale Faktoren, insbesondere durch menschliche Handlungen, und weniger durch technische Eigenschaften beeinflusst. Ein hochgradig anpassungsfähiges System kann seine Leistung im Vergleich zu vor der Störung entweder steigern oder stabil halten, selbst wenn der Druck auf das System zunimmt. Besonders relevant ist, dass in einem solchen System die Resilienz selbst als Reaktion auf Störungen zunimmt. Im Gegensatz zur Absorptions- und Wiederherstellungsfähigkeit, die sich auf aktuelle Störungen konzentrieren, fokussiert sich die Anpassungsfähigkeit darauf, die Kompetenz des Systems zu erhöhen, zukünftige Herausforderungen zu bewältigen[28]. Darüber hinaus spielt die Anpassungsfähigkeit auch bei

27 *Ouyang,* Structural Safety v. 36 2012, 23 (27).
28 *Rehak*, International Journal of Critical Infrastructure Protection 25 2019, 125, (126).

https://doi.org/10.5771/9783748963494-13 - am 23.01.2026, 02:27:29. https://www.inlibra.com/de/agb - Open Access -

anhaltenden, intensiven Störungen eine entscheidende Rolle, indem sie das System an neue Bedingungen anpasst.

4. Resilienzprinzipien

Den oben genannten grundlegenden Fähigkeiten resilienter Systeme lassen sich verschiedene Resilienzprinzipien zuordnen, wobei diese Zuordnung nicht immer eindeutig ist. Oft betrifft ein spezifisches Resilienzprinzip nicht ausschließlich eine der drei Systemfähigkeiten. Beispielsweise kann eine modulare Struktur zunächst die Verbreitung initialer Schadensauswirkungen innerhalb eines Systems begrenzen und somit die Absorptionsfähigkeit erhöhen, später jedoch auch den Wiederaufbau des ursprünglichen Leistungsniveaus unterstützen.

Tabelle 1 stellt die Beziehungen zwischen ausgewählten Resilienzprinzipien und den drei Fähigkeiten resilienter Systeme dar.[29] Dabei wird verdeutlicht, wie multifunktionale und interdisziplinäre Ansätze zur Verbesserung der Resilienz beitragen. Verbreitete Resilienzprinzipien sind beispielsweise Diversität, Modularität, Redundanz und Flexibilität. Diese Prinzipien können je nach Kontext und Art des Störereignisses unterschiedliche Rollen spielen. Beispielsweise trägt Diversität zur Anpassungsfähigkeit bei, indem sie eine Vielzahl von Reaktionsmöglichkeiten auf neue Herausforderungen bietet, während Redundanz die Absorptionsfähigkeit durch zusätzliche Kapazitäten stärkt.

29 *Mentges*, International Journal of Disaster Risk Reduction v. 96 2023, 103893 (103912).

https://doi.org/10.5771/9783748963494-13 - am 23.01.2026, 02:27:29. https://www.inlibra.com/de/agb - Open Access -

Tabelle 1: Der Zusammenhang zwischen Resilienzprinzipien und den drei Systemfähigkeiten (adaptiert).

		Systemfähigkeiten		
		Absorptions-fähigkeit	Wiederherstel-lungsfähigkeit	Anpassungs-fähigkeit
Ausgewählte Resilienzprinzipien	Robustheit	X		
	Redundanz	X		
	Diversität	X	X	X
	Modularität	X	X	
	Situationsbewusstsein	X	X	
	Überwachung	X	X	
	Ressourcenvielfalt	X	X	
	Wiederherstellbarkeit		X	
	Schnelligkeit		X	
	Graduelle Verschlechterung		X	
	Flexibilität	X	X	X
	Vorbereitungsfähigkeit	X	X	X
	Antizipationsvermögen	X	X	X
	Graduelle Erweiterbarkeit	X	X	X

III. Bewertung

Die Bewertung der Resilienz eines Systems ermöglichet die Bestimmung der Notwendigkeit von Anpassungen bzw. die Einschätzung deren Auswirkungen. Hierbei können generell die drei Methodenarten qualitativ, quantitativ und semi-quantitativ unterschieden werden. Qualitative Methoden konzentrieren sich auf das Verstehen sozialer Phänomene aus der Perspektive der beteiligten Akteure und nutzen unstrukturierte oder halbstrukturierte Daten wie Interviews und Beobachtungen, um tiefere Einblicke in menschliches Verhalten und soziale Prozesse zu gewinnen. Quantitative Methoden basieren auf der systematischen Sammlung und Analyse numerischer Daten, mit dem Ziel, Muster, Beziehungen und Kausalitäten zu identifizieren sowie Hypothesen zu testen. Semi-quantitative Methoden kombinieren qualitative und quantitative Ansätze, erfassen Daten, die so-

https://doi.org/10.5771/9783748963494-13 - am 23.01.2026, 02:27:29. https://www.inlibra.com/de/agb - Open Access -

wohl numerisch als auch beschreibend sein können, und verwenden häufig Skalen oder Rangordnungen, um schwer messbare Daten zu klassifizieren.

Verbreitet sind vor allem semi-quantitative und quantitative Methoden. Beispiele für Ersteres sind Resilience Assessment Grids[30] und Resilienzmatrizen[31]. Resilience Assessment Grids analysieren die zentralen Systemfähigkeiten anhand vorgegebener Kriterien und Skalen. Der Prozess umfasst die Identifikation relevanter Resilienzprinzipien, die Datenerhebung durch Interviews, Umfragen oder Beobachtungen und die Analyse der gesammelten Daten. Dabei werden sogenannte Resilienzprofile erstellt, wobei es sich um eine grafische Darstellung in Form von Spinnendiagrammen handelt, die eine visuelle Bewertung ermöglichen.

Eine Resilienzmatrix organisiert die Systemfähigkeiten in verschiedenen Domänen (z.B. physisch, informationell und kognitiv) über die zeitlichen Phasen einer Störung (z.B. Vorbereitung, Absorption, Erholung und Anpassung). Die Benutzer bewerten das System und seine kritischen Funktionen, indem sie verschiedene Resilienzprinzipien anhand von Indikatoren einschätzen, und tragen diese Werte in normalisierter Form die Resilienzmatrix ein. Abschließend können die entsprechenden Werte aggregiert werden, so dass ein initialer und oberflächlicher Vergleich der Resilienz verschiedener Systeme und Systemkonfigurationen ermöglich wird.

Ein Großteil der quantitativen Methoden zur Resilienzbewertung zielt darauf ab, den zeitlichen Verlauf der Performance des untersuchten Systems bzw. einzelner Systemfunktionen vor, während und nach einer Störung zu quantifizieren[32]. Dies reicht von einer eher simplen Bestimmung des Integrals der Performanz über die Zeit[33] bis hin zu umfangreichen Ansätzen, welche die verschiedenen zeitlichen Phasen formell beschreiben[34]. Andere

30 *Hollnagel*. RAG-the resilience assessment grid. Safety-II in practice: developing the resilience potentials: Routledge, 2017, 50.
31 *Rand/Kurth/Fleming/Linkov*, International Journal of Disaster Risk Reduction v. 42, 2020, 101310 (101312).
32 *Hosseini/Barker/Ramirez-Marquez*, Reliability Engineering and System Safety v. 145 2016, 47, (51).
33 *Zobel*, Int. Conf. on Information Systems for Crisis Response and Management 2010, 1, (3).
34 *Guillouët/Keszöcze, Sill Torres*, Resilience Week 2021, 1 (4).

https://doi.org/10.5771/9783748963494-13 - am 23.01.2026, 02:27:29. https://www.inlibra.com/de/agb - Open Access -

Ansätze verfolgen eine system-orientierte Sicht und erfassen das Systemverhalten bspw. über Simulationsmodelle[35] oder Fuzzy-Logik.[36]

IV. Vergleich Risiko und Resilienz

Ein zentraler Punkt beim Verständnis von Resilienz liegt in der Unterscheidung zwischen Ansätzen, die Risiken reduzieren, und solchen, die Resilienz aufbauen. Hierbei spielt die Unvorhersehbarkeit von Ereignissen eine maßgebliche Rolle: Risikominderungsstrategien zielen darauf ab, auf vorhersehbare Ereignisse zu reagieren, während Resilienzstrategien darauf fokussieren, ein System so zu stärken, dass es flexibel auf jegliche, auch unerwartete, Situationen reagieren kann[37]. Tatsächlich hat das wachsende Bewusstsein für unvorhersehbare und einzigartige Herausforderungen maßgeblich zur steigenden Bedeutung des Resilienzdenkens in der politischen Diskussion beigetragen[38].

Die unterschiedlichen Schwerpunkte dieser Ansätze bestimmen die verfolgten Strategien. Risikominderungsstrategien lassen sich in Prävention, d.h. die Reduzierung der Eintrittswahrscheinlichkeit schwerwiegender Gefahren, Vermeidung, d.h. die Vermeidung der Aussetzung gegenüber Gefahrenquellen, und Schutz, d.h. die Verringerung der Anfälligkeit von Systemen, unterteilen. Prävention und Vermeidung konzentrieren sich auf vorhersehbare Gefahren, und versuchen die Wahrscheinlichkeit des Eintritts dieser zu verringern. Damit werden beiden nicht zu den resilienzfördernden Strategien gezählt. Im Gegensatz dazu gibt es beim Schutz Überschneidungen mit Resilienzansätzen: In beiden Fällen zielen die jeweiligen Maßnahmen darauf ab, die Auswirkungen von Störereignissen zu verringern, indem Maßnahmen ergriffen werden, die die Systemfähigkeiten stärken[39]. Aus der Risikoperspektive wird gezielt die Verwundbarkeit gegenüber bestimmten Ereignissen reduziert, während aus der Resilienzperspektive die Fähigkeit zur Bewältigung beliebiger Ereignisse im Mittelpunkt steht. Es bleibt festzuhalten, dass Resilienzmaßnahmen, die darauf abzielen, ein Sys-

35 *Niemi/Skobiej/Kulev, Sill Torres*, Reliability Engineering and System Safety v. 242 2024, 109719 (109721).

36 *Gote*, Fuzzy-Logik basierte Methodik zur Vulnerabilitätsbewertung eines Containerterminals, Hochschule, Bremerhaven, 2022, 20.

37 *Park/Sharman/Rao,* MIS Quarterly, v. 39, 2013, 317, (320).

38 *Petersen/Lange/Theocharidou*, Reliability Engineering and System Safety, v. 199, 2020 106872 (106873).

39 *Mentges*, Fn. 30 (103930)

https://doi.org/10.5771/9783748963494-13 - am 23.01.2026, 02:27:29. https://www.inlibra.com/de/agb - Open Access -

tem gegen unvorhersehbare Störungen zu schützen, gleichzeitig auch den Schutz vor bekannten Risiken erhöhen. Im gleichen Sinne steigern risikozentrierte Schutzmaßnahmen, die auf bestimmte Bedrohungen abzielen, im Allgemeinen auch die Fähigkeit eines Systems, mit unvorhergesehenen Störungen umzugehen. Letztlich wird die Wirksamkeit beider proaktiven Maßnahmen in der Reaktion des Systems auf ein auftretendes Störereignis zusammenwirken.

Der konzeptionelle Unterschied zwischen Risiko- und Resilienzmanagement zeigt sich jedoch in den angewandten Methoden. Das Risikomanagement fokussiert sich auf spezifische Risiken, während das Resilienzmanagement die Aufrechterhaltung und Stärkung der Systemfähigkeiten in den Vordergrund stellt. Trotz ihrer unterschiedlichen Schwerpunkte und Ansätze verfolgen Risikominderung und Resilienzaufbau ein gemeinsames Ziel: die negativen Folgen von Störungen zu minimieren. Kombinierte Maßnahmen, die sowohl Risikominderung als auch Resilienzaufbau integrieren, sind daher besonders effektiv, da sie sowohl bekannte als auch unvorhersehbare Herausforderungen bewältigen, indem sie die Eintrittswahrscheinlichkeit von Risiken reduzieren und gleichzeitig die Fähigkeit zur Reaktion auf diese stärken.

E. Ansätze zur Erhöhung der Resilienz maritimer Kritischer Infrastrukturen

Maßnahmen zur Erhöhung der Resilienz maritimer Kritischer Infrastrukturen gegenüber physischen Bedrohungen orientieren sich an den im vorherigen Kapitel eingeführten Resilienzprinzipien und lassen sich in die Bereiche Multidimensionale Seeraumüberwachung, Lagebewusstsein, Schutzmaßnahmen und systemische Ansätze unterteilen.

I. Multi-dimensionale Seeraumüberwachung

Folgend dem Resilienzprinzip Überwachung bildet die multidimensionale Seeraumüberwachung eine wichtige Säule für eine resiliente maritime Kritische Infrastruktur. Dies beinhaltet eine Mischung aus Sensorsystemen und -plattformen, die der Überwachung aller maritimen Dimensionen (Meeresboden, Unterwasser, Wasseroberfläche, Luftraum, Cyberraum) dienen. Ziel ist es, Objekte, Personen, Umweltparameter (bspw. Wetter, Meeresdaten), Veränderungen an den Komponenten der Infrastrukturen sowie

https://doi.org/10.5771/9783748963494-13 - am 23.01.2026, 02:27:29. https://www.inlibra.com/de/agb - Open Access -

den Ablauf der Prozess in den Infrastrukturen (bspw. Wartung, Logistik) zu erfassen. Die Sensorsysteme lassen sich grob nach ihrem Einsatzraum einordnen, d.h. Wasseroberfläche/Luftraum, Unterwasser/Meeresboden und Cyberraum.

Im Bereich Wasseroberfläche/Luftraum existiert eine Vielzahl von Sensoren, welche vor allem im elektromagnetischen Spektrum arbeiten[40]. Hierzu gehören optische Sensoren, insbesondere optische Kameras und Lidar-Sensoren, Radar-Systeme, inklusive Over-The-Horizon-Radar und Synthetic Aperture Radar, sowie Hyper- und Multispektrale Sensorsysteme[41]. Ein im maritimen Raum weithin verbreitetes System ist das Automatic-Identification-System, ein automatisches Tracking-System, das in der Schifffahrt zur Identifizierung und Positionsbestimmung von Schiffen verwendet wird. Darüber hinaus werden auch kontextbezogene Informationsquellen verwendet. Hierzu gehören Human-Intelligence, d.h. die Informationsgewinnung durch menschliche Quellen, Signals-Intelligence, d.h. die Fernmelde- und Elektronische Aufklärung, sowie Open-Source-Intelligence, d.h. die Informationsgewinnung aus frei verfügbaren und offenen Quellen[42].

Im Unterwasserbereich sind auf Grund starker Dämpfungseffekte Sensoren aus dem elektromagnetischen Spektrum nur sehr begrenzt einsetzbar[43]. Daher kommt es in diesem Bereich vor allem zum Einsatz akustischer Systeme, insbesondere von Sonar-Systemen[44]. Diese umfassen aktive und passive Sonare, Seitensichtsonare, Fächerecholot und Synthetic-Aperture-Sonar. Von steigender Bedeutung sind Systeme, die Lichtwellenleiterkabel, welche zur Datenkommunikation verwendet werden, als Sensor einsetzen. Hierbei sind vor allem Distributed-Temperature-Sensing- und Distributed-Acoustic-Sensing -Systeme zu nennen[45].

Sensorsysteme zu Überwachung der Bereiche Wasseroberfläche/Luftraum sowie Unterwasser/Meeresboden können entweder fest installiert sein oder auf Sensorplattformen eingesetzt werden. Klassische Plattformen sind im maritimen Bereich Satelliten, bemannte Luftfahrzeuge (bspw. Flugzeuge, Hubschrauber) und bemannte Über- und Unterwasserfahrzeuge.

40 *Briguglio/Crupi*, Journal of Marine Science and Engineering v. 12 2024, 353 (354).
41 *Thombre*, IEEE Transactions on Intelligent Transportation Systems 23.1 2022, 64 (67).
42 *Crosston/Valli*, Cyber-Intelligence, and Security 2017, 68 (70).
43 *Wright,* International Journal on Marine Navigation and Safety of Sea Transportation v. 13 2019, 503 (505).
44 *Blondel/Murton*, Handbook of Seafloor Sonar Imagery, 1997, 5 ff.
45 *Duckworth/Ku.*, Society for Optics and Photonics Conference 2013, 87110G (87112G).

https://doi.org/10.5771/9783748963494-13 - am 23.01.2026, 02:27:29. https://www.inlibra.com/de/agb - Open Access -

Von zunehmender Bedeutung werden jedoch auch unbemannte Luftfahrzeuge (bspw. Drohnen und High-Altitude Platforms) sowie Über- und Unterwasserfahrzeuge.[46]

II. Lagebewusstsein

Das Lagebewusst folgt den Resilienzprinzipien Situationsbewusstsein und Antizipationsvermögen und umfasst vor allem Lösungen zur Sensordatenfusion und -analyse sowie zur Lagebilderstellung[47]. Ziel ist es, zum einen die Informationen der eingesetzten Sensorsysteme zusammenzuführen und die aktuelle Lage darzustellen. Darüber hinaus sollen durch die automatische Detektion, Klassifizierung und Identifikation von Objekten, weiterführende Informationen gewonnen werden. Hierbei kommt es vor allem zum Einsatz von Methoden des maschinellen Lernens. Dies ermöglicht unteranderem die Erkennung von Anomalien, bspw. untypischen Schiffsverhalten oder auffällige Objekte in der Nähe von Infrastrukturen. Von zunehmender Bedeutung sind antizipative Ansätze, welche eine Prognose darüber liefern, wie sich eine Situation entwickelt und ob es notwendig wird, auf diese Lage reagieren zu müssen.

III. Schutzmaßnahmen

Schutzmaßnahmen folgen im weitesten Sinn dem Resilienzprinzip Robustheit und dienen der Verhinderung eines Störereignisses bzw. der Reduzierung der Auswirkungen eines solchen Ereignisses. Wie in Abschnitt B dargelegt, schränkt die räumliche Ausdehnung im maritimen Raum solche Schutzmaßnahmen signifikant ein, insbesondere im Hinblick auf den proaktiven und reaktiven Einsatz von Sicherheitskräften, welche in vielen Fällen lange Interventionszeiten haben.

Im Falle von Schiffen, welche ein auffälliges Verhalten zeigen, erfolgt gewöhnlich ein Ansprechen per Funk. Durch diese Maßnahme können vor allem anthropogene Bedrohungen abgewendet werden, bei denen die Angreifer unerkannt bleiben möchten, bspw. im Falle von unrechtmäßigen Aktivitäten staatlicher oder privater Akteure (z.B. Spionage oder Diebstahl).

46 *Soldi*, IEEE Aerospace and Electronic Systems Magazine v. 38 2013, 4 (5).
47 *Flenker/Stoppe*, Workshop on Maritime Systems Resilience and Security 2021, 1 (3).

https://doi.org/10.5771/9783748963494-13 - am 23.01.2026, 02:27:29. https://www.inlibra.com/de/agb - Open Access -

Im maritimen Raum gewinnen semi-automatische und automatische Drohnenabwehrsysteme in den drei Dimensionen Unterwasser, Wasseroberfläche und Luft an Bedeutung[48]. Unterwasserabwehrsysteme schützen vor unbemannten Unterwasserfahrzeugen, die bspw. Kabel und Anlagen angreifen könnten. Auf der Wasseroberfläche und in der Luft bieten Anti-Drohnen-Technologien Schutz vor maritimen Drohnen und Luft-Drohnen, die für Spionage, Sabotage oder Angriffe genutzt werden können. Diese integrierten Systeme ermöglichen die Echtzeit-Erkennung und ggf. Neutralisierung von Bedrohungen.

Eine weitere Maßnahme sind schwimmende Barrieren und Unterwassernetze[49]. Erstere sind kettenartige Strukturen aus Stahl, Beton und anderen Materialien, die über Schäkeln und Drehgelenke miteinander verbunden sind und Schutz vor Booten oder U-Booten bieten. Unterwassernetze, aus haltbarem Stahldraht und am Meeresboden verankert, dienen als physische Barrieren mit Sensoren zur Erkennung von Eindringlingen. Auf Grund der räumlichen Ausdehnung vieler maritimer Infrastrukturen, bspw. Offshore Windparks und Pipelines, sind solche Barrieren jedoch nur begrenzt einsetzbar.

IV. Systemische Ansätze

Systemische Ansätze zur Erhöhung der Resilienz maritimer Systeme gegenüber physischen Bedrohungen umfassen vor allem Maßnahmen mit dem Fokus auf Absorptionsfähigkeit, die im Vorfeld eines Ereignisses relevant sind, sowie auf Wiederherstellungsfähigkeit, die im Nachgang eines erfolgreichen Angriffs von Bedeutung ist. Hierzu gehören vor allem Redundanzmaßnahmen und Reparaturfähigkeiten. Erstere umfassen bspw. die Verlegung mehrere Unterseekabel, wobei eine räumliche Trennung angestrebt werden sollte, oder die redundante Auslegung zentraler Komponenten in Offshore Plattformen, so dass die Auswirkungen eines Ausfalls einzelner Elemente verringert werden können.

Die Reparaturfähigkeit zerstörter Systeme und Komponenten kann durch eine Vielzahl von Maßnahmen gesteigert werden. Bei Unterseekabeln ist es ratsam, Kabellegerschiffe bereitzuhalten, die abhängig von deren Verfügbarkeit, der Entfernung und Tiefe des beschädigten Kabels sowie den

48 *Yaacoub/Noura/Salman/Chehab*, Internet of Things v. 11 2020, 100218 (100241).
49 *Knysh*, Ocean Engineering v. 227 2021, 108707 (108710).

https://doi.org/10.5771/9783748963494-13 - am 23.01.2026, 02:27:29. https://www.inlibra.com/de/agb - Open Access -

aktuellen Witterungsbedingungen eine Reparatur ermöglichen. Zusätzliche Maßnahmen umfassen die Vorratshaltung kritischer Ersatzteile sowie die Etablierung von Lieferketten und Vereinbarungen mit Herstellern und Lieferanten, um eine schnelle Beschaffung von Ersatzteilen zu gewährleisten. Es ist jedoch zu berücksichtigen, dass viele kritische Elemente maritimer Infrastrukturen groß und kostspielig sind, wie beispielsweise die Transformatoren von Offshore-Konverterstationen.

F. Fazit

Maritime Infrastrukturen sind von teils entscheidender Bedeutung für ein Land, sowohl für die Wirtschaft als auch für die Energieversorgung, so dass eine größere Anzahl dieser Systeme als Kritische Infrastruktur gelten. Der Schutz dieser Infrastrukturen ist aufgrund vielfältiger Bedrohungen, wie Naturkatastrophen und von Menschen ausgehende Gefahren, äußerst anspruchsvoll und komplex. Hinzu kommt die räumliche Ausdehnung der zu überwachenden Gebiete und die langen Interventionszeiten der Sicherheitskräfte. Resilienz, also die Fähigkeit von Systemen, Störereignissen standzuhalten und dabei ihre Funktionsfähigkeit entweder zu bewahren oder zeitnah wiederherzustellen, ist daher von entscheidender Bedeutung. Maßnahmen zur Erhöhung der Resilienz maritimer Infrastrukturen reichen von multidimensionaler Überwachung und Situationsbewusstsein bis hin zu Schutzmaßnahmen und systemischen Ansätzen. Dabei ist es wichtig, diese Maßnahmen ganzheitlich zu betrachten und umzusetzen, um eine nachhaltige Sicherheit und Widerstandsfähigkeit der maritimen Infrastrukturen zu gewährleisten.

https://doi.org/10.5771/9783748963494-13 - am 23.01.2026, 02:27:29. https://www.inlibra.com/de/agb - Open Access -